www.istatistikciler.org
İstatistikçiler Dergisi 3 (2010) 45-53

İstatistikçiler Dergisi

Galois cisimleri ve en yüksek çözümlü 2^{k-1} tasarımlarının oluşturulması

Nazan Danacıoğlu

Sinop Üniversitesi
Fen-Ed. Fak. İstatistik Bölümü
Osmaniye Köyü Yeni Cezaevi Yanı
57000 Sinop, Türkiye
nazand@sinop.edu.tr

F. Zehra Muluk

Başkent Üniversitesi
Ticari Bilimler Fak.
Sigortacılık ve Risk Yönetimi Bölümü
06810 Ankara, Türkiye
zmuluk@baskent.edu.tr

Özet

Kesirli çok etkenli tasarımları, uygulamada yaygın olarak kullanılmaktadır. Bu çalışmada, sonlu cisim teorisinden, Galois cisimleri üzerindeki polinomlardan yararlanarak, en yüksek çözümlü 2^{k-1}tasarımlarının nasıl oluşturulabileceği gösterilmiştir.

Anahtar sözcükler: Çok etkenli tasarımlar; Kesirli çok etkenli tasarımlar; Sonlu cisimler; Galois cismi; Polinomlar.

Abstract

Galois Fields And Construction of 2^{k-1} Designs with Highest Resolution

Fractional factorialdesigns are commonly used in practice. In this article, the finite flelds theory and polynomials over Galois fields were used to design 2^{k-1} designs with highest resolution.

Keywords: *Factorial designs; Fractional factorial designs; Finite fileds; Galois field; Polynomials.*

1. Giriş

Çok etkenli ve kesirli çok etkenli (KÇE) (fractional factorial designs) tasarım teorisinde pek çok sorun; geometrik, cebirsel ya da birleşimsel (combinatorial) yapıya dönüşür. Sonuç olarak; gruplar, halkalar (rings), cisimler (fields), Öklid ve izdüşümsel (projective) geometri gibi sonlu matematiksel yapılar, çok etkenli ve KÇE tasarımlarla ilgili pek çok sorunun çözümünde, genelleştirilmesinde ve aydınlatılmasında başarıyla kullanılmaktadır.

Çok etkenli tasarımları oluşturma yöntemlerinden literatürde bulunan bazıları; dikey dizimler (orthogonal arrays), sonlu geometriler (finite geometries), cebirsel ayrışma (algebraic decomposition), etki karışımı (confounding), Hadamard matrisleri ve sonlu grafikler olarak sıralanabilir.

KÇE tasarımların cebirsel yapısı bugüne kadar pek çok çalışmada yer almıştır. Shirakura, Suetsugu ve Tsuji [10], Hadamard matris ve Galois cisminden (GF) (Galois field) yaralanarak 2^m tasarımları oluşturma yöntemi önermişler; Pistone and Rogartin [9], KÇE tasarımlarda, düzey kodları için cebirsel istatistikleri incelemiş, Xu [13], GF, doğrusal kodlar ve izdüşümsel geometriden yararlanarak KÇE tasarımlar için bir algoritma oluşturmuşlardır.

Bu çalışmada, katsayıları GF üzerinde bulunan polinomlardan yararlanarak, çok etkenli tasarımlar ve bunların en yüksek çözümlü yarı kesirlerine nasıl ulaşılacağıyla ilgilenilmiştir.

2. Genel bilgiler

Bilindiği gibi, etkenlerin p düzeyli olduğu bir KÇE tasarım, p büyüklüğünde GF kullanılarak oluşturulabilir ve p asal bir sayı olduğunda, sonlu cisim aritmetiği, p modülünde tam sayı aritmetiğine eşittir. Bu nedenle modüler aritmetik ile ilgili bazı tanımlar üzerinde durulacaktır:

2.1. Denklikler ve Euler ϕ fonksiyonu

Tanım 1. $n > 0$ ve $a, b \in Z$ olsun. Eğer $n \mid a-b$ (n, a-b yi böler) ise, a sayısı n modülüne göre b'ye denktir denir ve $a \equiv b \pmod{n}$ şeklinde gösterilir [6].

Tanım 2. $x \equiv a \pmod{n}$ gibi bir denklik bağıntısı için n tane denklik sınıfı vardır ve her biri $\bar{0}, \bar{1}, ..., \overline{n-1}$ sınıflarından birine eşittir. Bu denklik sınıflarının açık olarak yazılımı;

$$\bar{0} = \{0, \pm n, \pm 2n, ...\},$$

$$\bar{1} = \{1, 1 \pm n, 1 \pm 2n, ...\}$$

$$\vdots \qquad (1)$$

$$\overline{n-1} = \{n-1, (n-1) \pm n, (n-1) \pm 2n, ...\}$$

şeklindedir ve n modülüne göre kalan sınıfları olarak adlandırılır.

$$Z_n = \{\bar{0}, \bar{1}, \bar{2}, ..., \overline{n-1}\}$$

kümesine, n modülüne göre kalan sınıflarının kümesi denir [3].

p asal bir sayı olmak üzere, Z_p'nin p-1 tane sıfırdan farklı her öğesi tersinirdir (p asal olduğunda, Z_p'nin sıfırdan farklı her öğesinin Z_p içinde bir tersi vardır). Tanım 3, rastgele bir n>1 tam sayısı için Z_n'nin tersinir öğelerinin sayısını bulmaya yöneliktir [6].

Tanım 3. n>1 için, Z_n içindeki tersinir öğelerin sayısı $\Phi(n)$ ile gösterilir ve $n \rightarrow \Phi(n)$ bağıntısına ya da kısaca $\Phi(n)$'ye Euler fonksiyonu denir [1,6].

$\Phi(n)$ ile gösterilen sayı; Z_n'nin öğelerinden, n'den küçük ya da eşit olup, n ile aralarında asal olan tam sayıların sayısıdır. Örneğin, $\Phi(8)=4$'tür; çünkü, $\bar{1}, \bar{3}, \bar{5}, \bar{7}$, 8 ile aralarında asaldır.

Özellik 1. (Euler**)** n, $a \in Z$ ve n>0 olsun. (n,a)=1 ise, $a^{\Phi(n)} \equiv 1 \pmod{n}$'dir [6].

Sonuç 1. (Fermat) p, $a \in Z$ olsun. p asal ve $p \nmid a$ (p, a'yı bölmez) ise, $a^{p-1} \equiv 1 \pmod{p}$'dir [4].

Sonuç 2. (Fermat) p asal ise, her $a \in Z$ için, $a^p \equiv a \pmod{p}$'dir [4].

2.2.Sonlu cisimler

Gerçel sayılar, rasyonel sayılar ve kompleks sayılar cisimlere örnek olarak verilebilir ve her biri sonsuz sayıda elemana sahiptir. Sadece, sonlu sayıda eleman içeren bir cisim, sonlu cisim (finite field) olarak adlandırılır. Örneğin, n tamsayı modülü Z_n ile gösterildiğinde, mod n'de yapılan standart toplama ve çarpma işlemlerine göre, Z_n sonlu bir cisimdir [11,12].

Teorem 1. Z_n yalnız ve yalnız n asal sayı ise sonlu bir cisimdir.

Tanım 4. F bir cisim olsun. F cisminin karakteristiği; $\sum_{i=1}^{m} 1 = 1 + 1 + \ldots + 1 = 0$ eşitliğini sağlayan en küçük pozitif m tamsayısıdır. Eğer m yoksa, karakteristik 0 olarak tanımlanır [11].

Teorem 2. F, p karakteristiğine sahip sonlu bir cisimse, bu durumda F, n pozitif tamsayısı için, p^n elemanlıdır.

F, q elemanlı sonlu bir cisimse, genellikle GF(q) ile gösterilir ve q elemanlı GF olarak adlandırılır. Buradaki q, p^n biçimindedir ve bir asal sayı ya da asal sayının kuvvetidir. GF(p^n), p karakteristikli bir cisimdir ve Z_p cismi, GF(p) olarak gösterilir [3, 11].

2.2.1. Galois cismi

p bir asalsa, $F_p = <F_p , +_p , ._p >$ sistemi, $F_p = \{0, 1, 2, \ldots, p-1\}$ olmak üzere, bir GF'dir ve GF(p) ile gösterilir. Gerçekte, F_p , en basit GF'dir [3].

Tanım 5. r, $x^r = 1$ yapan en küçük pozitif tamsayı olsun. Bu durumda r, x'in derecesidir ve r en büyük değeri, p-1'i aldığında; x'e GF(p)'nin *ilkel elemanı* (primitive element) denir. Her GF(p)'de ilkel bir eleman vardır. x ilkel elemansa, GF(p)'nin sıfır olmayan bütün elemanları, aşağıdaki diziye dahildir [3].

$$x^0 = 1, x, x^2, \ldots, x^{p-2} \qquad (2)$$

Tanım 6. GF(p)[x], $a_i\}$ katsayıları GF(p) cisminde olan, rastgele dereceli $a_0 + a_1x + a_2x^2 + \ldots + a_{n-1}x^{n-1}$, $a_i \in \{0,1\}$, polinomlarının birleşimidir [7].

Tanım 7. GF(p)[x]'de düşük dereceden polinomların çarpımı şeklinde yazılamayan f(x) fonksiyonuna, GF(p)'de indirgenemez denir [3,7].

f(x), GF(p)'de indirgenemezse, GF(p^n)'nin elemanlarını oluşturmak için en küçük fonksiyondur. En küçük fonksiyon f(x) uygun olarak seçilirse; x ile gösterilen sınıf, GF(p^n)'nin *ilkel elemanı* olacaktır ve bu durumda, GF(p^n)'nin sıfır olmayan bütün elemanları aşağıdaki gibi ifade edilebilir.

$$x^0 = 1, x, x^2, \ldots, x^{p^n-2} \qquad (3)$$

Eşitlik (3)'teki ifade, x'in güç döngüsü (power cycle) olarak adlandırılır. Bazı güç döngüleri Çizelge 1'de verilmektedir [3].

GF(2^2) için güç döngüsü oluşturulsun. GF(2^2)'nin cisim elemanları bulunurken, Tanım 6'dan, derecesi n=1 olan bir polinomdan yararlanılır.

$p(x) = a_0 + a_1x$ ya da $p(x) = a_1x + a_0$, $a_i \in Z$, $i=0,1$, $a_1 \neq 0$ olmak üzere;

$$\begin{array}{llll} p(x)= & a_1x & + & a_0 \\ & 0 & & 0 \quad \rightarrow 0 \\ & 0 & & 1 \quad \rightarrow 1 \\ & 1 & & 0 \quad \rightarrow x \\ & 1 & & 1 \quad \rightarrow x+1 \end{array} \qquad (4)$$

dir. *GF(2^2) için* Çizelge 1'de verilen en küçük polinom, $1+x+x^2$'dir ve Tanım 7'den, aynı zamanda indirgenemez bir polinomdur (Bkz. Çiz. 2) olarak gösterilmiştir. Eşitlik (3)'teki güç döngüsü kullanıldığında;

$$x^0 = 1, x, x^2, ..., x^{p^n-2} \rightarrow 1, x, x^{2^2-2} = x^2 \rightarrow 1, x, x^2$$

elde edilir. Ancak $x^2 \equiv x+1 \pmod{x^2+x+1}$ olduğundan, güç döngüsü;

$$1, x, x+1 \qquad (5)$$

olacaktır. Görüldüğü gibi, cismin 0 dışındaki elemanları, güç döngüsünü oluşturmaktadır.

Çizelge 1. Bazı GF(2^n) cisimleri için en küçük polinomlar ve güç döngüleri

p^n	**En küçük polinom**	**Güç döngüsü**
2^2	x^2+x+1	1,x,x+1
2^3	x^3+x^2+1	1,x,x^2, x^2+1, x^2+x+1,x+1,x^2+x
2^4	x^4+x^3+1	1,x, x^2, x^3, x^3+1, x^3+x+1, x^3+x^2+x+1, x^2+x+1, x^3+x^2+x, x^2+1, x^3+x, x^3+x^2+1,x+1, x^2+x, x^3+x^2

GF(2^3) için güç döngüsü oluşturulsun. Tanım 6'dan, GF(2^3)'ün elemanları bulunurken, derecesi n=2 olan bir polinomdan yararlanılır. $p(x)= a_2x^2 + a_1x + a_0$, $a_i \in Z$, i=0,1, $a_1 \neq 0$ olmak üzere;

$$\begin{array}{llll} p(x)= & a_2x^2 + & a_1x + & a_0 \\ & 0 & 0 & 0 \quad \rightarrow 0 \\ & 0 & 0 & 1 \quad \rightarrow 1 \\ & 0 & 1 & 0 \quad \rightarrow x \\ & 0 & 1 & 1 \quad \rightarrow x+1 \\ & 1 & 0 & 0 \quad \rightarrow x^2 \\ & 1 & 0 & 1 \quad \rightarrow x^2+1 \\ & 1 & 1 & 0 \quad \rightarrow x^2+x \\ & 1 & 1 & 1 \quad \rightarrow x^2+x+1 \end{array} \qquad (6)$$

elde edilir ki, GF(2^3) için, Çizelge 2.2'de verilen en küçük fonksiyon x^3+x^2+1 kullanılarak, Eşitlik (3)'ten bulunan güç döngüsü; $x^0 = 1, x, x^2, ..., x^{p^n-2} \rightarrow 1, x, x^2, x^3, x^4, x^5, x^6$ olmak üzere,

$$1,\ x,\ x^2,\ x^2+1, x^2+x+1, x+1, x^2+x \qquad (7)$$

dir (Bkz. Çiz. 2).

GF(2^4) için güç döngüsü oluşturulsun. GF(2^4)'ün elemanları bulunurken, derecesi n=3 olan bir polinomdan yararlanılır. $p(x)= a_3x^3 + a_2x^2 + a_1x + a_0$, $a_i \in Z$, i=0,1, $a_3 \neq 0$ olmak üzere,

$p(x)= a_3x^3 +$	$a_2x^2 +$	$a_1x +$	a_0	
0	0	0	0	$\rightarrow 0$
0	0	0	1	$\rightarrow 1$
0	0	1	0	$\rightarrow x$
0	0	1	1	$\rightarrow x+1$
0	1	0	0	$\rightarrow x^2$
0	1	0	1	$\rightarrow x^2+1$
0	1	1	0	$\rightarrow x^2+x$
0	1	1	1	$\rightarrow x^2+x+1$
1	0	0	0	$\rightarrow x^3$
1	0	0	1	$\rightarrow x^3+1$
1	0	1	0	$\rightarrow x^3+x$
1	0	1	1	$\rightarrow x^3+x+1$
1	1	0	0	$\rightarrow x^3+x^2$
1	1	0	1	$\rightarrow x^3+x^2+1$
1	1	1	0	$\rightarrow x^3+x^2+x$
1	1	1	1	$\rightarrow x^3+x^2+x+1$

(8)

elde edilir. Çizelge 1'deki $x^4 + x^3 +1$ en küçük fonksiyonu kullanılarak Eşitlik (3)'ten güç döngüsü;

$x^0 = 1, x, x^2, ..., x^{p^n-2} \rightarrow 1, x, x^2, x^3, x^4, x^5, x^6, x^7, x^8, x^9, x^{10}, x^{11}, x^{12}, x^{13}, x^{14}$'tür.

$$1, x, x^2, x^3, x^3+1, x^3+x+1, x^3+x^2+x+1, x^2+x+1, x^3+x^2+x,$$
$$x^2+1, x^3+x, x^3+x^2+1, x+1, x^2+x, x^3+x^2 \quad (9)$$

dir ve Çizelge 1'den de görülebilir.

2.2.2. İndirgenemez polinomlar

Bilindiği üzere, p^n elemanlı bir cisim oluşturmak için, GF(p)[x]'de n. dereceden bir indirgenemez polinoma ihtiyaç vardır. Asıl sorun, GF(p)[x]'de her pozitif n sayısı için, n. dereceden bir polinomun olup olmadığıdır. Gerçekte bakılması gereken, monik bir indirgenemez polinomdur. Monik polinom, x'in en yüksek kuvvetinin sıfır olmayan katsayısı 1 demektir [13].

Tanım 8. (2 ya da 3. dereceler için indirgenebilirlik testi) F bir cisim olsun. $f(x)\in F[x]$ ve $degf(x)=2$ ya da 3 ise; f(x), yalnız ve yalnız F'de sıfır değerini alıyorsa, F'de indirgenebilirdir [4].

Örneğin, $1+x+x^3$, Z_2'de indirgenemezdir; çünkü, Z_2'de $0^3 + 0 + 1\neq 0$ ve $1^3 + 1 + 1\neq 0$'dır.

Sonuç 3. Herhangi bir $p\geq 2$ asal için,

$$\varphi_p(x)=\frac{x^p-1}{x-1}=x^{p-1}+x^{p-2}+...+x+1, \in Z[x] \quad (10)$$

Q (rasyonel sayılar) üzerinde ve dolayısıyla Z'de indirgenemezdir [4].

Çizelge 2'de, mod 2 için, dereceleri n=1'den 5'e kadar olan indirgenemez polinomlar listelenmektedir [3].

Çizelge 2. Mod 2'de n. dereceden indirgenemez polinomlar

n	**İndirgenemez polinomlar**
1	$1+x$, x
2	$1+x+x^2$
3	$1+x+x^3$, $1+x^2+x^3$
4	$1+x+x^4$, $1+x+x^2+x^3+x^4$, $1+x^3+x^4$
5	$1+x^2+x^5$, $1+x+x^2+x^3+x^5$, $1+x^3+x^5$, $1+x+x^3+x^4+x^5$, $1+x^2+x^3+x^4+x^5$, $1+x+x^2+x^4+x^5$

2.2.2. En küçük polinom

Tanım 9. F, p karakteristikli bir cisim olsun ve F^* 0 olmayan cisim elemanlarını göstersin. $\alpha \in F^*$ olsun. GF(q)'ya göre α'nın en küçük polinomu m(x)'dir ve $m(\alpha) = 0$'dır [7].

Tanım 10. Bir α elemanının en küçük polinomu tektir [5].

Teorem 3. $\alpha \in F^*$ için, α'nın en küçük polinomu $m_\alpha(x)$, indirgenemezdir ve $m_\alpha(x) \mid x^q$-x'tir [5,7].

Tanım 11. $\alpha \in F$ için, t, $\alpha^{p^t} = \alpha$ yapan en küçük pozitif tamsayı olsun. GF(q)'ya göre α'nın çekimler (conjugates) kümesi;

$$C(\alpha) = \left\{ \alpha, \alpha^p, \alpha^{p^2}, ..., \alpha^{p^{t-1}} \right\} \tag{11}$$

ve p karakteristikli F cisminde, bütün i'ler için, $C(\alpha) = C\left(\alpha^{p^i}\right)$'dir [5,11].

Teorem 4. F, p karakteristikli bir cisim ve $\alpha \in F^*$ olsun. $C(\alpha)$, GF(q)'ya göre α'nın çekimler kümesi olduğunda,

$$m_\beta(x) = \prod_{\beta \in C(\alpha)} (x - \beta) \tag{12}$$

katsayıları GF(q) üzerinde β'nın en küçük polinomudur [11].

$F=GF(2^2)$ cismi oluşturulsun**.** Öncelikle, Z_2'de indirgenemez kübik bir polinoma ihtiyaç vardır ve Çizelge 2'den, $f(x)= x^2 + x +1$ alınmıştır. F'nin elemanları; {[0], [1], [x], [1+x]}(Bkz. Eş.4) ve karakteristiği de 2'dir (Bkz. Tanım 4). Elemanların çarpımları f(x) polinom modundadır. $x^2 + x +1 \equiv 0 \pmod{f(x)}$ ve Eşitlik (1)'den Z_2'de $1 \equiv -1$ olduğundan, $x^2 \equiv -x-1 = x+1 \pmod{f(x)}$'dir.

α=x, F'nin ilkel elemanı ya da üretecidir. Gerçekte, Tanım 5'ten, bu cisim için 1 dışındaki 0 olmayan her eleman (Bkz. Eş.5), cismin üretecidir.

Tanım 11'den $\alpha^{p^t} = \alpha$ yapan en küçük eleman; $x^2 \equiv x+1 \pmod{x^2+x+1}$, $x^4 = x$ ya da $\alpha^{2^2} = \alpha$, olduğundan 2'dir. Eşitlik (11)'den çekimler kümesi; $C(\alpha) = \left\{ \alpha, \alpha^2 \right\}$'dir. Eşitlik (12)'deki en küçük polinom için, karışıklık olmaması amacıyla x yerine y kullanılırsa,

$$m_\beta(y) = \prod_{\delta \in C(\beta)} (y - \delta)$$

şeklinde yazılabilir. Eşitlik (4) ve (5)'ten, $\beta = (10) = \alpha^1$ alınsın.

$$m_\beta(y) = \prod_{\delta \in C(\beta)} (y - \delta) = (y - \beta)(y - \beta^2) = y^2 + y(\beta^2 + \beta) + \beta^3 \quad (13)$$

$(\beta^2 + \beta) = (\alpha^2 + \alpha) = (x + 1 + x) = 1$ olduğundan, en küçük polinom, $m_\beta(y) = y^2 + y + 1$'dir.

Çizelge 3'te GF(2^3)'ün elemanlarının en küçük polinomları, 1 üreteç için verilmektedir [2].

Çizelge 3. En küçük polinomu $f(x)=x^3 + x^2 + 1$ alınan GF(2^3) cismi

GF(2^3) cismi için $f(x)=x^3 + x^2 + 1$ ve $\alpha=x$ alındığında	
$\beta=(010) = x = \alpha^1$ $\beta=(100) = x^2 = \alpha^2$ $\beta=(111) = x^2+x+1 = \alpha^4$	$m_\beta(y)= y^3 + y^2 + 1$
$\beta=(101) = 1+x^2 = \alpha^3$ $\beta=(011) = x + 1 = \alpha^5$ $\beta=(110) = x^2+x = \alpha^6$	$m_\beta(y)= y^3 + y + 1$

Çizelge 2'de Z_2'de indirgenemez diğer bir kübik polinom $f(x)= x^3+x+1$ alındığında, GF (2^3) elemanları ve karşılık gelen en küçük polinomları da bulunmuştur (Bkz. [2]).

Çizelge 3'te verilen ve GF(2^3)'ü oluştururken kullanılan en küçük polinomların her biri, x^8-x'i bölmelidir ve derecelerinin toplamı 8 olmalıdır (Bkz. Teo.3). GF(2^3) için,

$$x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1) \quad (14)$$

dir. $\alpha=x$ olduğunda en küçük polinomlar; x, x+1, (x^3+x+1), (x^3+x^2+1)'dir.

3. 2^{k-1} Tasarımları

Bilindiği üzere, 2^{k-p} deneme içeren bir 2^k tasarımına, 2^k tasarımının $1 / 2^p$ kesiri ya da 2^{k-p} KÇE tasarımı denir. Burada; k: etken sayısı, p: üreteç ya da tanımlayıcı bağıntı sayısıdır. Bu düzen için tanımlayıcı bağıntı yapısı (defining constrast pattern), başlangıçta seçilen p tane üreteç ve bunların 2^p - p -1 tane genelleştirilmiş etkileşiminden (generalized interaction) oluşur. p=1 olduğunda, çok etkenli bir tasarımın yarı kesrine karşılık gelir [8].

KÇE tasarımın çözümü (resolution) ise, tanımlayıcı bağıntı yapısındaki en kısa kelime uzunluğu olarak tanımlanabilir ve burada, Romen rakamıyla, alt indis olarak gösterilmiştir.

Tanımlayıcı bağıntısı I=ABC olan 2^{3-1}_{III} KÇE tasarımı Çizelge 4'te gösterilmektedir.

Çizelge 4. 2^{3-1}_{III} Tasarımı (I=ABC)

a	b	c=a+b	Denemeler
0	0	0	000
0	1	1	011
1	0	1	101
1	1	0	110

Bu tasarımın tanımlayıcı bağıntısı, $I=ABC= x^2+x+1=(111)$ olarak da gösterilebilir. x^2+x+1 GF(2^3)'ün elemanıdır (Bkz. Eş. 5) ve indirgenemez bir en küçük polinomdur (Bkz. Çiz. 1 ve Çiz. 2).

Teorem 3 ve Sonuç 3'ten, $m_\alpha(x) = x^2+x+1 \mid x^4-x$ 'dir. Başka bir deyişle,

$$x^4 - x = x(x+1)(x^2+x+1)$$

ve

$$x^3 - 1 = (x+1)(x^2+x+1) \qquad (15)$$

olduğu söylenebilir. x^2+x+1, aynı zamanda en küçük polinomdur. x ve x+1 ise $GF(2^3)$'ün 1. dereceden en küçük polinomlarıdır.

Eşitlik (4)'te verilen $GF(2^2)$'nin elemanları, Çizelge 4'te a ve b sütunlarıyla gösterilen tamamlanmış 2^2 çok etkenli tasarımına karşılık gelmektedir. 2^{3-1} tasarımına, yani 2^2 çok etkenlisinin yarı kesrine ulaşmak için, bir anlamda, $GF(2^3)$'ün yarı kesri elde edilmelidir. Bunun için, Eşitlik (15)'te tanımlayıcı bağıntıyı gösteren polinom dışındaki x+1 polinomundan yararlanılabilir. $GF(2^3)$'ün yarı kesri ya da 2^{3-1} tasarımı Çizelge 5'te gösterilmiştir.

Çizelge 5. $GF(2^2)$'den elde edilen 2^{3-1}_{III} tasarımı

$GF(2^2)$	$x^3 - 1 = (x+1)(x^2+x+1)$	Elemanların (x+1) polinomuyla çarpımı	2^{3-1}_{III} tasarımının denemeleri
0 0 (0)	(x+1)	0.x+1=0	0 0 0
0 1 (1)	(x+1)	1. (x+1)=x+1	0 1 1
1 0 (x)	(x+1)	x(x+1)=x^2+x	1 1 0
1 1 (x+1)	(x+1)	(x+1)(x+1)= x^2+1	1 0 1

Çizelge 5'te son sütundaki denemeler polinom derecesine göre sıralanırsa, Çizelge 4'ün son sütunundaki deneme sırasına ulaşılabilir.

Çizelge 6'da, I=ABCDE=(11111)=$x^4+x^3+x^2+x+1$ tanımlayıcı bağıntılı 2^{5-1}_{V} tasarımının nasıl oluşturulduğu gösterilmektedir.

Çizelge 6. $GF(2^4)$'ten elde edilen 2^{5-1}_{V} tasarımı

$GF(2^4)$	Elemanların (x+1) polinomuyla çarpımı	2^{5-1}_{V} tasarımının denemeleri
0 0 0 0 (0)	0. (x+1)= 0	0 0 0 0 0
0 0 0 1 (1)	1. (x+1)= x+1	0 0 0 1 1
0 0 1 0 (x)	x. (x+1)= x^2 +x	0 0 1 1 0
0 0 1 1 (x+1)	(x+1).(x+1)= x^2+1	0 0 1 0 1
0 1 0 0 (x^2)	x^2.(x+1)= x^3 + x^2	0 1 1 0 0
0 1 0 1 (x^2+1)	(x^2+1).(x+1)= x^3+x^2+x+1	0 1 1 1 1
0 1 1 0 (x^2+x)	(x^2+x).(x+1)= x^3+x	0 1 0 1 0
0 1 1 1 (x^2+x+1)	(x^2+x+1) (x+1)= x^3+1	0 1 0 0 1
1 0 0 0 (x^3)	x^3.(x+1)= x^4+x^3	1 1 0 0 0
1 0 0 1 (x^3+1)	(x^3+1).(x+1)= x^4+x^3+x+1	1 1 0 1 1
1 0 1 0 (x^3+x)	(x^3+x).(x+1)= x^4+x^3+x^2+x	1 1 1 1 0
1 0 1 1 (x^3+x+1)	(x^3+x+1).(x+1)= x^4+x^3+x^2+1	1 1 1 0 1
1 1 0 0 (x^3+x^2)	(x^3+x^2).(x+1)= x^4+x^2	1 0 1 0 0
1 1 0 1 (x^3+x^2+1)	(x^3+x^2+1).(x+1)= x^4+x^2+x+1	1 0 1 1 1
1 1 1 0 (x^3+x^2+x)	(x^3+x^2+x).(x+1)= x^4+x	1 0 0 1 0
1 1 1 1 (x^3+x^2+x+1)	(x^3+x^2+x+1).(x+1)= x^4+1	1 0 0 0 1

Sonuç 3'ten $x^4+x^3+x^2+x+1$ polinomu indirgenemezdir ve $GF(2^5)$'in elemanıdır. Teorem 3'ten, $m_\alpha(x) = x^4+x^3+x^2+x+1 \mid x^5-x$ 'dir. Buradan,

$$x^5 - 1 = (x+1)\left(x^4 + x^3 + x^2 + x + 1\right)$$

yazılabilir. Böylelikle, Eşitlik 8'de verilen GF(2^4) elemanlarının (x+1) polinomuyla çarpılması sonucu 2_V^{5-1} tasarımının denemelerine ulaşılmıştır (Bkz. Çiz. 6).

4. Sonuç ve öneriler

Bilindiği üzere, KÇE, özellikle 2-düzeyli tasarımlar (2^{k-p}), belli etkileşimlerin olmadığı-önemsiz olduğu-varsayımının yapılabildiği durumlarda; sadece etkenlerden bazılarının önemli olduğu düşünülen ön (screening) çalışmalarda yararlı olup, uygulamada yaygın olarak kullanılmaktadır. Bir 2^{k-p} KÇE tasarımının mümkün en yüksek çözüme sahip olması istenir.

Bu çalışmada, 2^{k-p} tasarımlarında p=1 olduğu zaman, en yüksek çözümlü yarı kesirli tasarımlara GF kullanılarak ulaşılmıştır. Burada yer verilmeyen diğer yarı kesirler de aynı şekilde elde edilebilmektedir. MATLAB programının GF fonksiyonlarını kullanarak en küçük polinomlara, polinom köklerine veya GF elemanlarına ulaşmak mümkündür. Polinom çarpımlarının el ile yapılması zor olduğunda MATLAB programından yararlanılabilir. Etken sayısı çift olduğunda, örneğin, 2_{IV}^{4-1} tasarımı oluşturulmak istenirse, p asal olmadığından Sonuç 3 sağlanmamaktadır. Bu tasarım için tanımlayıcı bağıntı I=ABCD= x^3+x^2+x+1'dir ve polinom GF(2^3)'te indirgenebilir bir polinomdur (Bkz. Tanım 8). Buna rağmen, $x^4-1=(1+x)(x^3+x^2+x+1)$ olduğunda, verilen yöntem kullanılarak oluşturulabilmektedir. Yarı tekrarlar dışındaki KÇE tasarımlar için polinomların matrislerle gösterimi gerekecektir.

Danacıoğlu [2], Hamming kodlarında yer alan, üreteç matrisi (generator matrix) ve denklik-kontrol matrislerini (parity-control matrix) kullanarak, KÇE tasarımlara ulaşmış ve tasarımların kod karşılıklarını bulmuştur.

Xu [13], r=n-k olmak üzere, GF(2)'deki sıfır olmayan $(u_1, \ldots u_r)^T$ r kümeden oluşan $r\times(2^r-1)$ boyutlu G matris olduğunda; düzenli (regular) her 2^{n-k} KÇE tasarımının n sütununun GF(2)'deki G'nin bütün satır kombinasyonlarından oluşan bir $2^r\times(2^r-1)$ matrisi olarak düşünülebileceğini belirtmiştir.

Kaynaklar

[1] F. Çallıalp, (1999), *Sayılar Teorisi*, İstanbul.
[2] N. Danacıoğlu, (2005), *Kesirli Çok Etkenli Deneylerde Çözüm ve En Az Sapma Kavramı,* H.Ü. İstatistik Bölümü Doktora Tezi.
[3] A. Dey, (1985), *Orthogonal Fractional Factorial Designs*, New Delhi, Wiley Eastern.
[4] J. A. Gallian, (1986), *Contemporary Abstract Algebra*, D.C.Health and Company.
[5] W. C. Huffman, V. Pless, (2003), *Fundemantals of Error Correcting Codes*, Cambridge University Pres.
[6] A. Kaya, (1988), *Sayılar Kuramına Giriş*, İzmir.
[7] A. J. Menezes, S. A. Vanstone, P. C. Oorschot van, (1997), *Handbook of Applied Cryptography*, CRC Pres.
[8] D. C. Montgomery, (1984), *Design and Analysis of Experiments, Second Edition*, John Wiley&Sons, NY.
[9] G. Pistone, M. P. Rogartin, (2007), Algebraic Statistics of Level Codings for Fractional Factorial Designs, *Journal of Statistical Plann. and Inf.,*138, 234-244.
[10] T. Shirakura, T. Suetsugu, T. Tsuji, (2002), Constructions of Main Effect Plus Two Plans for 2^m Factorials, *Journal of Statistical Plann. and Inf*., 105, 405-415.
[11] S. A. Vanstone, P. C. Oorschot van, (1989), *An Introduction to Error-Correcting Codes with Application,s* Kluwer Academic Publishers.
[12] D. Wiggert, 1978, *Error-Control Coding and Applications*, Artech House.
[13] H. Xu, (2009), Algorithm construction of efficient fractional factorial designs with large sizes, *Technometrics*, 51,3,262-277.