



SONLU CİSİMLER ÜZERİNDE YENİ ÖZ-ORTOGONAL KOD AİLELERİ

Melike Çakmak^{1,*}, Ahmet Sınak², Oğuz Yayla¹

¹Orta Doğu Teknik Üniversitesi, Uygulamalı Matematik Enstitüsü, Kriptografi Anabilim Dalı, Ankara, Türkiye

²Akdeniz Üniversitesi, Sosyal Ve Beşeri Bilimler Fakültesi, Yönetim Bilişim Sistemleri Bölümü, Antalya, Türkiye

ÖZET

Bir doğrusal kod, eğer kendi dual kodu içerisinde yer alıyorsa, öz-ortogonal kabul edilir. Öz-ortogonal kodlar, doğrusal tamamlayıcı dual kodlar ve kuantum kodlar dahil olmak üzere çeşitli uygulamalara sahiptir. Doğrusal kodlar inşa etmenin çeşitli yöntemleri vardır ve bu yöntemlerden biri sonlu cisimler üzerinde tanımlı fonksiyonların kullanılmasıdır. Ding ve arkadaşları [1], $\mathcal{C}_D = \{(\text{Tr}_p^m(bd_1), \text{Tr}_p^m(bd_2), \dots, \text{Tr}_p^m(bd_n)) : b \in \mathbb{F}_{p^m}\}$, formunda doğrusal kodlar üreten inşa yöntemini önermişlerdir, burada $D = \{d_1, d_2, \dots, d_n\}$ tanımlayıcı kümedir. Bu durumda $\mathcal{C}_D$, uzunluğu n ve boyutu en fazla m olan $\mathbb{F}_p$ üzerinde tanımlı bir doğrusal koddur. Bu inşa yöntemi kullanılarak iyi parametrelere sahip birçok doğrusal kod üretilmiştir. Bu yaklaşımla, uygun şekilde seçilen tanımlayıcı kümelerle, $\mathbb{F}_p$ üzerinde zayıf düzenli bükük ve plato fonksiyonları kullanılarak az sayıda ağırlığa sahip çeşitli iyi kodlar elde edilmiştir. Yakın zamanda, Heng ve arkadaşları [2], $\mathcal{C}_D$ kodunun genişletilmiş hâli olan $\overline{\mathcal{C}_D} = \{(\text{Tr}_p^m(bd_1), \text{Tr}_p^m(bd_2), \dots, \text{Tr}_p^m(bd_n)) + c\mathbf{1} : b \in \mathbb{F}_{p^m} \text{ ve } c \in \mathbb{F}_p\}$ kodunu inceleyerek üçlü ve p -mertebeli öz-ortogonal kod aileleri elde etmişlerdir, burada $\mathbf{1} = (1, 1, \dots, 1) \in \mathbb{F}_p^m$ sabit vektör ve f zayıf düzenli bükük bir fonksiyondur. Ayrıca, bu öz-ortogonal kodlardan yola çıkarak yeni üçlü LCD kodları inşa etmişlerdir. Bu çalışmada, [2, 3] tarafından yapılan son çalışmalardan ilham alınarak, tanımlayıcı küme $D_\theta = \{x \in \mathbb{F}_{p^m} : f(x) + \theta = 0\}$ temel alınarak, zayıf düzenli plato dengeli fonksiyonlardan genişletilmiş kod $\overline{\mathcal{C}_{D_\theta}}$ inşa edilmiştir. Bu inşa sonucunda, beş ağırlıklı ve altı ağırlıklı $\mathbb{F}_p$ üzerinde tanımlı öz-ortogonal doğrusal kodlar elde edilmiştir. Ayrıca, bu öz-ortogonal kodlarla ilişkili dual kodların parametreleri açık bir şekilde belirlenmiştir. Bu çalışma birinci yazarın Orta Doğu Teknik Üniversitesi, Kriptografi Anabilim Dalında ikinci ve üçüncü yazarın danışmanlığı ile yürütülen tez çalışmasının sonuçlarını içerir.

Anahtar Kelimeler 1. Öz-ortogonal kod, 2. Doğrusal tamamlayıcı dual kod, 3. Zayıf düzenli plato fonksiyonu

Kaynaklar

- [1] Ding, Kelan, and Cunsheng Ding. "A class of two-weight and three-weight codes and their applications in secret sharing." IEEE Transactions on Information Theory 61.11 (2015): 5835-5842.
- [2] Heng, Ziling, Dexiang Li, and Fenjin Liu. "Ternary self-orthogonal codes from weakly regular bent functions and their application in LCD codes." Designs, Codes and Cryptography 91.12 (2023): 3953-3976.
- [3] Chen, Wenbing, Jindeng Zhang, and Minjia Shi. "A new family of p-ary self-orthogonal code from weakly regular plateaued functions." Journal of Applied Mathematics and Computing 71.2 (2025): 2327-2348.

*Sorumlu Yazarın E-postası: mcakmak@metu.edu.tr