Sonlu Cisimler ve Sonlu Halkalar Üzerinde Bazı Uygulamalar

Proje No: 107T826

Prof. Dr. Ferruh Özbudak

ŞUBAT 2011
ANKARA

Önsöz

Bu araştırma projesinde, sonlu cisim aritmetiği, kimlik doğrulama kodları, çok katlı döngüsel kodlar, sonlu cisimler üzerinde özyineleme bağıntıları ve diziler, cebirsel geometrinin kodlama teorisine uygulamaları ve sonlu cisimler üzerinde diğer bir takım uygulamalar çalışılmıştır. Elde edilen sonuçlar uluslararası dergilerde yayınlanmış ayrıca ulusal ve uluslararası bilimsel toplantılarda sunulmuş ve bu toplantıların bildirilerinde yayınlanmıştır. Proje kapsamında yapılan yayınların sayısı yirmi dörttür.

Projeden alınan mali destek ile proje yürütücüsü, araştırmacılar ve busriyerler yurtiçi ve yurtdışı çeşitli bilimsel toplantılara katılmış ve bu sayede benzer konularda araştırma yapan bilim insanları ile tanışmış, fikir alışverişinde bulunmuş ve gelecekte olası yeni projeler için irtibat kurmuşlardır.

Bu proje, ODTÜ matematik bölümünde yürütülmüş ve ODTÜ matematik bölümü tarafından desteklenmiştir. Ayrıca ODTÜ uygulamalı matematik enstitüsünün kriptografi bölümü de bu projeye destek vermiştir.

İçindekiler

Özet

1950 li yıllardan itibaren, haberleşme gizliliği ve güvenilirliği için cebirsel yapıların kullanılmasının önemi anlaşılmış ve özellikle sonlu cisimler kullanılarak çeşitli amaçlar için uygulamalar geliştirilmiştir. Bunların yanında bilim adamları 1990'lardan beri Galois halkalarının da bu alanlara ilginç uygulamaları olabileceğini göstermiştir. Bu projede, sonlu cisimler ve Galois halkaları üzerinde bahsi geçen uygulamalar farklı bakış açıları ile çalışılmıştır.

Çalışılan konulardan biri sonlu cisim aritmetiğidir. Çalışmalarımız, bu konuda en önemli başlıklardan biri olan polinom çarpması üzerinde yoğunlaşmıştır. Hesaplamaları daha verimli gerçekleştirebilmek için yeni polninom çarpımı metodları geliştirilmiştir. Bulduğumuz metodlar ya olan metodlar kadar ya da onlardan da daha verimli oldular.

Sonlu cisimler ve sonlu halkalarda lineer kodlar üzerine çalışıldı. Asimptotik olarak iyi parametrelere sahip lineer kodlar incelendi. Karakteristiği p olan alfabeler üzerinde, uzunluğu p^s ve $2p^s$ olan bütün döngüsel kodların Hamming mesafeleri bulundu. Ayrıca fonksiyon cisimlerinin teorisi kullanılarak kimlik doğrulama kodları ve bu kodların güvenliği çalışıldı.

Sonlu cisimler üzerinde lineer özyineleme bağıntılarının karmaşıklıkları incelendi. Çoklu dizilerin karmaşıklıkları üzerine istatiksel sonuçlar elde edildi.

Anahtar kelimeler: sonlu cisimler, sonlu halkalar, sonlu cisim aritmetiği, polinom çarpımı, cebirsel fonksiyon cisimleri, lineer kodlar, kodlama teorisi, kriptografi, döngüsel kodlar, kimlik doğrulama kodları, özyineleme bağıntıları, sonlu cisimler üzerinde diziler, lineer karmaşıklık.

Abstract

Since 1950's, the importance of the use of algebraic structures for communication secrecy and reliability is becoming more and more important and in particular, there have been many models based on finite fields for several purposes. In addition to this, since the mid 1990's, researchers realized that Galois rings have also important and interesting applications on these areas. In this project, such applications on Finite Fields and Finite Rings were studied in different aspects.

We studied finite field arithmetic. We mainly focused on polynomial multiplication which is a crucial part of this area. Using the theory of function fields, we developed algorithms to perform efficient polynomial multiplication over finite fields. In some cases, our methods are as good as the existing ones and in some other cases they are better than the previous ones in terms of computational complexity.

We studied linear codes over finite fields and Galois rings. We studied asymptotically good linear codes coming from algebraic geometric constructions. We determined the Hamming distance of all linear codes of length p^s and $2p^s$ over a an alphabet of characteristic p. Using linear codes and algebraic function fields, we introduced new authentication codes and studied their security.

We studied the linear complexity of linear recurring sequences over finite fields. We also studied the joint linear complexity of linear recurring multisequences from a statistical point of view.

Keywords: finite fields, finite rings, finite field arithmetic, polynomial multiplication, algebraic function fields, linear codes, coding thoery, cryptography, cyclic codes, authentication codes, recurrence relations, sequences over finite fields,linear complexity.

Giriş

Proje kapsamında sonlu cisimler ve sonlu halkalar üzerinde kodlama teorisi ve kriptografi için çeşitli uygulamalar çalışılmıştır. Bunun için projenin başında detaylı bir literatür taraması yapılmış ve *Yöntem* başlığı altında verilen eserler incelenemiş ve yeni teknikler öğrenilmiştir. Daha sonra bu teknikler kullanılarak, çoğunluğu tez yöneticisinin projede bursiyer olan doktora öğrencileri ile beraber yürüttüğü araştırmalarda, çeşitli sonuçlar elde edilmiş ve projenin kalan kısmında bu sonuçlar makale ve konferans bildirisi olarak derlenmiştir. Yapılan yayınlar *Bulgular* başlığı altında anlatılmıştır.

Çalışılan 6 alt başlık ve içerikleri şöyledir.

Sonlu Cisim Aritmetiği

Haberleşme ve şifreleme uygulamalarının büyük çoğunluğu sonlu cisimler üzerinde işlem yapmayı gerektirmektedir. Bu işlemlerin verimli bir şekilde yaılması uygulamalar açısından büyük önem taşımaktadır. Bu sebeple özellikle 80'li yıllardan itibaren yüksek verimli sonlu cisim aritmetiği üzerine yapılan çalışmaların sayısı artmıştır. Bu işlemler için özellikle polinom çarpımının verimli yapılması gerekmektedir. Bu projede, sonlu cisimler üzerindeki fonksiyon cisimlerinin ve cebirsel eğrilerin teorisi kullanılarak, bazı durumlarda önceki bilinen metodlar kadar iyi sonuç veren alternatif metodlar ve bazı durumlarda da bilinen metodlardan daha yüksek verimliliğe sahip çarpım metodları geliştirilmiştir.

Kimlik Doğrulama Kodları

Günümüz haberlşeme sistemlerinde gelen mesajın gerçekten de doğru kaynaktan gelip gelmediği ve mesaj iletilirken üçüncü şahıslar tarafından değiştirilip değiştirilmediği soruları son derece önemlidir ve pek çok araştırmacı tarafından çalışılmıştır. Lineer kodlar kullanarak kimlik doğrulama ve veri bütünlüğü doğrulama sistemleri geliştirmek mümkündür. Bu projede, cebirsel eğrilerin teorisini de kullanarak, kimlik doğrulama sistemlerinde kullanılacak lineer kodlar ve burada sisteme yapılacak çeşitli saldırıların başarı olasılıkları çalışılmıştır.

Çok Katlı Döngüsel Kodlar

Lineer kodların bir alt kümesi olan döngüsel kodlar uygulamalarda sağladığı kolaylık ve cebirsel yapıları itibarı ile hep çok ilgi ceken ve üzerinde araştırma yapılan bir konu olmuştur. Şimdiye kadar yapılan çalışmaların büyük çoğunluğunda uzunluğu sonlu cismin karakteristiği tarafından bölünmeyen kodlar çalışılmıştır. Bu projede ise uzunluğu alfabenin karakteristiğinin bir kuvveti veya bir kuvvetinin iki katı olan döngüsel kodlar calışılmıştır. Bu kodların Hamming mesafeleri bulunmuştur.

Sonlu Cisimler Üzerinde Özyineleme Bağıntıları ve Diziler

Sonlu cisimler üzerinde özyineleme bağıntıları akan şifre sistemlerinin matematiksel temelini oluşturmaktadır. Bu dizilerin lineer karmaşıklıkları, karşılık gelen şifreleme sistemlerinin güvenliği için en önemli ölçütlerdendir. Bu projede çoklu dizilerin genellenmiş ortak doğrusal karmaşıklığı istatiksel olarak incelenmiştir.

Cebirsel Geometrinin Kodlama Teorisine Uygulamaları

Cebirsel geometrik kodların asimptotik olarak çok iyi parametrelere sahip olabilecekleri gösterildikten sonra cebirsel geometrinin kodlama teorisine olan uygulamaları büyük önem kazanmıştır. Bu projede asimptotik olarak iyi özelliklere sahip olan cebirsel geometrik kodlar hakkında günümüze kadar yapılan çalışmalar incelenmiş ayrıca cebirsel geometrik argümanlar kullanarak çeşitli kodların parametreleri için üst değerler elde edilmiştir.

Diğer Çalışmalar

Yukarıdakı çalışmaların yanında lineer kodlar ve ortagonal diziler arasındaki ilişkiler, sır paylaşım sistemleri ve politoplar kullanarak indirgenemeyen polinomlar bulma üzerine çalışmalar yapılmıştır.

Yöntem

Çalışmalar için [Boztaş and Kumar, 1994], [Helleseth et al., 2007], [Ness and Helleseth, 2006], [Tang et al., 2005b], [Tang et al., 2005a], [Gilbert et al., 1974], [Ding and Niederreiter, 2004], [Özbudak and Saygi, 2006], [Özbudak and Saygi, 2006], [Sarkar and Stinson, 2001], [Stinson et al., 2000a], [Stinson and Wei, 2004], [Stinson et al., 2000b], [Wang and Xing, 2001], [Liu and Shen, 2006], [Montgomery, 2005], [Dinh and López-Permouth, 2004], [Dinh, 2005], [Dinh, 2006], [Dinh, 2007], [Dinh, 2008] makaleleri incelendi ve öğrenilen teknikler uygulandı.

Bulgular

Elde edilen sonuçlar makale, konferans bildirisi ve konferans bildiri özeti olarak yayınlanmıştır. Giriş bölümünde bahsedilen başlıklara göre bu yayınlar gruplandırılarak aşağıda anlatılmıştır.

Sonlu cisim aritmetiği üzerine şu yayınlar yapılmıştır.

[Cenk and Özbudak, 2008] çalışmasında, Çinli kalan teoremi üzerine geliştirilen bir teknik ile karakteristiği 3 olan bazı sonlu cisim aileleri için çarpma işleminin karmaşıklığı (multiplicative complexity) geliştirilmiştir. Ayrıca $\mathbb{F}_{3^{6\cdot 97}}$ cismi için çarpım formülleri açıkça belirlenmiştir.

[Cenk and Özbudak, 2010] makalesinde sonlu cisimler üzerindeki eğrilerin teorisi kullanılarak, $q = 2, 3, 4$, $2 \leq n \leq 18$ durumlarında, $\mathbb{F}_{q^n}$ sonlu cisimlerindeki çarpma işlemi için bilineer karmaşıklığı ya bilinen en iyi değerler ya da onlardan daha iyi olan yöntemler geliştirilmiştir.

[Cenk and Özbudak, 2009b] makalesinde iki elemanlı sonlu cisimler üzerindeki n-terimli polinomların çarpım karmaşıklığı için iyi bir üst sınır elde edilmiş ve bu yöntem kullanılarak terim sayısı az olan polinom çarpımlarının belli durumlarında bilinen en iyi çarpım metodları elde edilmiştir.

[Cenk et al., 2009] çalışmasında cisim uzantıları, polinom interpolasyonu ve Toom-Cook metodu kullanılarak, belli durumlarda, bilinen yöntemlerden daha iyi polinom çarpımı yöntemleri elde edilmiştir.

[Cenk and Özbudak, 2009a] bildirisinde $\mathbb{F}_{5^{5n}}$ sonlu cisminde polinom çarpımları özel durumlarda geliştirilmiştir.

[Akleylek et al.,] çalışmasında Montgomery çarpımındaki ön fazı gerçekleştirmeden sonlu cisimler üzerinde daha hızlı polinom çarpımı yapılabileceği gösterilmiştir. Ayrıca bu çarpımın az sayıda devre elemanı ile yapılabileceği gösterilmiştir.

[Akleylek et al., 2010a] bildirisinde kesikli Fourier dönüşümü kullanılarak bir polinom çarpım metodu bulunmuştur. Bu metod belli durumlarda, bilinen yollardan daha iyi sonuçlar vermektedir.

[Akleylek et al., 2010b] bildirisinde, karakteristiği iki olan sonlu cisim elemanları için Charlier polinomları kullanılarak yeni bir gösterim bulunmuştur. Bu gösterim

ile yapılan polinom çarpması ve polinom modulosuna indirgeme işlemlerinin daha verimli yapılabileceği gösterilmiştir.

[Akleylek et al., 2011] makalesinde Chebyshev formundaki polinomların çarpımı çalışılmıştır. Bu formdaki polinomların çarpımı için verimli bir çarpma algoritması bulunmuş ve bu algoritmanın bir takım durumlarda, bilinen algoritmalardan daha verimli olduğu gözlenmiştir.

[Akleylek and Özbudak, 2011] makalesinde sonlu cisim elemanlarının, verimli aritmetik için, bir gösterim biçimi çalışılmıştır. Bu gösterim biçimi ile çarpma işlemini yapan devrelerde kullanılan XOR ve AND elemanlarının sayısı azaltılabilmektedir.

Kimlik doğrulama kodları üzerine şu yayınlar yapılmıştır.

[Özbudak et al., 2009] bildirisinde cebirsel fonksiyon cisimlerindeki rasyonel nokta sayıları kullanılarak doğrulama kodları çalışılmıştır. Bu kodlar kullanılarak oluşturulan sistemler için bazı atakların başarı olasılıkları belirlenmiştir.

[Özbudak et al., 2011] makalesinde gizliliği olan doğrulama kodları incelenmiştir. Çeşitli atakların başarı olasılıkları bulunmuştur. Bululnan doğrulama kodları, kullanılan fonksiyonlar mükemmel lineer olmadığı kimi durumda da, iyi parametrelere sahiptir.

Çok katlı döngüsel kodlar üzerine şu yayınlar yapılmıştır.

[Özadam and Özbudak, 2009] makalesinde p^s uzunluğundaki döngüsel lineer kodların Hamming mesafesinin [Dinh, 2008] çalışmasında belirtildiğinden çok daha basit ve kısa bir yol ile bulunabileceği gösterilmiştir.

[Özadam and Özbudak, 2009] bildirisinde karakteristiği p olan cisimler üzerinde, $2p^s$ uzunluğundaki bütün döngüsel kodların Hamming mesafesi bulunmuştur.

Sonlu cisimler üzerinde özyineleme bağıntıları ve diziler üzerine şu yayınlar yapılmıştır.

[Meidl and Özbudak, 2008] bildirisinde sonlu cisimler üzerindeki çoklu dizilerin ortak doğrusal karmaşıklığı incelenmiştir. Bu dizilerin karmaşıklıkları akan şifre uygulamalarının güvenliği için önem oluşturmaktadır. Bu çalışmada, bu dizilerin ortak lineer karmaşıklığı (joint linear complexity) ile genelleştirilmiş ortak lineer karmaşıklıkları arasındaki ilişkiler incelenmiştir.

[Meidl and Özbudak, 2009] makalesinde çoklu dizilerin genellenmiş ortak lineer karmaşıklıgı istatiksel olarak incelenmiştir. Bu dizilerin karmaşıklığının beklenen değeri ve varyansı belirlenmiştir.

[Fu et al., 2009] makalesinde karakteristik polinomlarına göre çoklu diziler incelenmiş ve bu polinomların çarpanlarına göre lineer karmaşıklıklarının varyansı ve beklenen değeri ifade edilmiştir.

[Çalık et al., 2010] makalesinde lineer olmayan geri beslemeli kayan sayaçlar incelenmiştir. Bu sistemlerin en yüksek döngüye sahip olması için bazı yeni gerekli koşullar bulunmuştur.

Cebirsel geometrinin kodlama teorisine uygulamaları üzerine şu yayınlar yapılmıştır.

[Niederreiter and Özbudak, 2008] makalesinde asimptotik olarak parametreleri bilinen en iyi değerlerin üstüne çıkan cebirsel geometrik kodlar incelenmiştir.

[Güneri and Özbudak, 2008] makalesinde Weil-Serre tarzı sınırlar kullanarak sonlu cisimler üzerindeki lineer kodların Hamming ağırlıklarına üst değer bulmak için yeni bir metod geliştirilmiştir. Elde edilen bu üst değerin bazı durumlarda BCH üst değerinden daha iyi sonuçlar verdiği gözlenmiştir.

Diğer çalışmalar üzerine şu yayınlar yapılmıştır.

[Sezer and Özbudak, 2008] bildirisinde ortogonal diziler ile lineer kodlar arasındaki ikili ilişki kullanılarak parametreleri bazı uç sınır değerlerine erişen optimal sonsuz lineer kod kümeleri elde edilmiştir.

[Koyuncu and Özbudak, 2009] makalesinde cisimler üzerinde sonsuz elemanlı indirgenemeyen çok değişkenli polinom kümeleri elde edilmiştir. Bunun için integral olarak indirgenemeyen politoplar kullanılmıştır.

[Koyuncu and Özbudak, 2011] makalesinde politop metodu kullanılarak, cisimler üzerinde çok değişkenli polinomların mutlak indirgenemez olma olasılıları çalışılmıştır.

[Kaşkaloğlu and Özbudak, 2010] çalışmasında hiyerarşik eşik sır paylaşım sistemleri için alternatif sistemler bulunmuştur.

Sonuç

Proje kapsamında elde edilen en ilginç sonuçlardan bir tanesi, fonksiyon cisimleri ve cebirsel eğrilerin teorisi kullanılarak elde edilen polinom çarpımı metodlarının pek çok durumda ya bilinen sonuçlar kadar iyi olduğu ya da onlardan bile daha verimli olduğudur. Proje süresince, bu konuda ODTÜ uygulamalı matematik enstitüsü bünyesinde bir araştırma grubu kurulmuştur. Ayrıca konu üzerine doktora dersleri açılmış ve bu grubun büyütülmesi amaçlanmıştır. Uluslararası düzeyde nitelikli araştırma yapacak durumdaki bu grup ile çalışmalara devam edilmesi düşünülmektedir.

Daha önce çok katlı dongüsel kodlar fazla çalışılmamıştır. Bu kodlar üzerinde ilginç teknikler öğrenilmiş ve belli durumlarda bu kodların ideal yapısı ve Hamming mesafeleri belirlenmiştir. Gelecekte, çok katlı lineer kodlar teorisinde elde edilen sonuçların farklı halkalara ve daha genel durumlara genellenmesi amaçlanmaktadır.

Sonlu cisimler üzerinde özyineleme bağıntılarının lineer karmaşıklığı üzerine elde edilen istatiksel sonuçlar bizi bu sonuçların halkalar durumunda da doğru olup olmayacağı sorusunun cevabını bulmaya teşvik etmiştir. Gelecekte bu konuda çalışmalar yapılması planlanmaktadır.

Cebirsel geometrinin, kodların asimptotik davranışlarının yanında sonlu cisim aritmetiği ve lineer kodlara çok ilginç uygulamaları olduğu gözlenmiştir. Cebirsel geometrinin kodlama teorisine uygulamaları için daha fazla literatür taraması yapılması ve farklı teknikler öğrenilmesi ve ileride bunların daha farklı şekillerde uygulamalarının araştırılması düşünülmektedir.

Referanslar

[Akleylek et al.,] Akleylek, S., Cenk, M., and Özbudak, F. Faster montgomery modular multiplication without pre-computational phase for some classes of finite fields. In *Proceedings of the 25th International Symposium on Computer and Information Sciences (ISCIS 2010), to appear*, volume 62.

[Akleylek et al., 2010a] Akleylek, S., Cenk, M., and Özbudak, F. (2010a). Modified discrete fourier transform for efficient polynomial multiplication. In *Proceedings of the 4th International Conference on Information Security and Cryptology (ISC-TURKEY 2010)*.

[Akleylek et al., 2010b] Akleylek, S., Cenk, M., and Özbudak, F. (2010b). Polynomial multiplication over binary fields using charlier polynomial representation with low space complexity. In *Proceedings of INDOCRYPT 2010*, volume 6498 of *Lecture Notes in Comput. Sci.*, pages 227–237. Springer, Berlin.

[Akleylek et al., 2011] Akleylek, S., Cenk, M., and Özbudak, F. (2011). On the polynomial multiplication in chebyshev form. *IEEE Transactions on Computers, accepted for publication*.

[Akleylek and Özbudak, 2011] Akleylek, S. and Özbudak, F. (2011). Modified redundant representation for designing arithmetic circuits with small complexity. *IEEE Transactions on Computers, accepted for publication*.

[Boztaş and Kumar, 1994] Boztaş, S. and Kumar, P. (1994). Binary sequences with gold-like correlation but larger linear span. *IEEE Transactions On Information Theory*, 40(2):532–537.

[Çalık et al., 2010] Çalık, c., Turan, M. S., and Özbudak, F. (2010). On feedback functions of maximum length nonlinear feedback shift registers. *IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences*, E93A(6):1226–1231.

[Cenk et al., 2009] Cenk, M., Koç, c. K., and Özbudak, F. (2009). Polynomial multiplication over finite fields using field extensions and interpolation. In Bruguera, J., Cornea, M., DasSarma, D., and Harrison, J., editors, *ARITH: 2009 19TH IEEE International Symposium On Computer Arithmetic*, Proceedings - Symposium on Computer Arithmetic, pages 84–91. IEEE COMPUTER SOC.

[Cenk and Özbudak, 2008] Cenk, M. and Özbudak, F. (2008). Efficient multiplication in $\mathbb{F}_{3^{lm}}$, $m \geq 1$ and $5 \leq l \leq 18$. In *Progress in cryptology—AFRICACRYPT 2008*, volume 5023 of *Lecture Notes in Comput. Sci.*, pages 406–414. Springer, Berlin.

[Cenk and Özbudak, 2009a] Cenk, M. and Özbudak, F. (2009a). Efficient multiplication in finite fields of characteristic 3 and 5 for pairing based cryptography. In *Information Security Conference*.

[Cenk and Özbudak, 2009b] Cenk, M. and Özbudak, F. (2009b). Improved polynomial multiplication formulas over f-2 using chinese remainder theorem. *IEEE Transactions On Computers*, 58(4):572–576.

[Cenk and Özbudak, 2010] Cenk, M. and Özbudak, F. (2010). On multiplication in finite fields. *J. Complexity*, 26(2):172–186.

[Ding and Niederreiter, 2004] Ding, C. and Niederreiter, H. (2004). Systematic authentication codes from highly nonlinear functions. *IEEE Trans. Inform. Theory*, 50(10):2421–2428.

[Dinh, 2005] Dinh, H. Q. (2005). Negacyclic codes of length 2^s over Galois rings. *IEEE Trans. Inform. Theory*, 51(12):4252–4262.

[Dinh, 2006] Dinh, H. Q. (2006). Repeated-root constacyclic codes of length 2^s over $\mathbb{Z}_{2^a}$. In *Algebra and its applications*, volume 419 of *Contemp. Math.*, pages 95–110. Amer. Math. Soc., Providence, RI.

[Dinh, 2007] Dinh, H. Q. (2007). Complete distances of all negacyclic codes of length 2^s over $\mathbb{Z}_{2^a}$. *IEEE Trans. Inform. Theory*, 53(1):147–161.

[Dinh, 2008] Dinh, H. Q. (2008). On the linear ordering of some classes of negacyclic and cyclic codes and their distance distributions. *Finite Fields Appl.*, 14(1):22–40.

[Dinh and López-Permouth, 2004] Dinh, H. Q. and López-Permouth, S. R. (2004). Cyclic and negacyclic codes over finite chain rings. *IEEE Trans. Inform. Theory*, 50(8):1728–1744.

[Fu et al., 2009] Fu, F.-W., Niederreiter, H., and Özbudak, F. (2009). Joint linear complexity of arbitrary multisequences consisting of linear recurring sequences. *Finite Fields Appl.*, 15(4):475–496.

[Gilbert et al., 1974] Gilbert, E. N., MacWilliams, F. J., and Sloane, N. J. A. (1974). Codes which detect deception. *Bell System Tech. J.*, 53:405–424.

[Güneri and Özbudak, 2008] Güneri, C. and Özbudak, F. (2008). Weil-Serre type bounds for cyclic codes. *IEEE Trans. Inform. Theory*, 54(12):5381–5395.

[Helleseth et al., 2007] Helleseth, T., Kholosha, A., and Ness, G. J. (2007). Characterization of m-sequences of lengths $2^{2k}-1$ and 2^k-1 with three-valued cross correlation. *IEEE Trans. Inform. Theory*, 53(6):2236–2245.

[Kaşkaloğlu and Özbudak, 2010] Kaşkaloğlu, K. and Özbudak, F. (2010). On hierarchical threshold access structures. In *Proceedings of Information Systems Technology Panel Symposium, IST-091/RSY-021.*

[Koyuncu and Özbudak, 2009] Koyuncu, F. and Özbudak, F. (2009). Integral and homothetic indecomposability with applications to irreducibility of polynomials. *Turkish J. Math.*, 33(3):283–294.

[Koyuncu and Özbudak, 2011] Koyuncu, F. and Özbudak, F. (2011). Probabilities for absolute irreducibility of multivariate polynomials by the polytope method. *Turkish Journal of Mathematics, accepted for publication.*

[Liu and Shen, 2006] Liu, L. and Shen, H. (2006). Explicit constructions of separating hash families from algebraic curves over finite fields. *Des. Codes Cryptogr.*, 41(2):221–233.

[Meidl and Özbudak, 2008] Meidl, W. and Özbudak, F. (2008). Generalized joint linear complexity of linear recurring multisequences. In *Sequences and their applications—SETA 2008*, volume 5203 of *Lecture Notes in Comput. Sci.*, pages 266–277. Springer, Berlin.

[Meidl and Özbudak, 2009] Meidl, W. and Özbudak, F. (2009). Linear complexity over $\mathbb{F}_q$ and over $\mathbb{F}_{q^m}$ for linear recurring sequences. *Finite Fields Appl.*, 15(1):110–124.

[Montgomery, 2005] Montgomery, P. (2005). Five, six, and seven-term karatsuba-like formulae. *IEEE Transactions On Computers*, 54(3):362–369.

[Ness and Helleseth, 2006] Ness, G. J. and Helleseth, T. (2006). A new three-valued cross correlation between m-sequences of different lengths. *IEEE Trans. Inform. Theory*, 52(10):4695–4701.

[Niederreiter and Özbudak, 2008] Niederreiter, H. and Özbudak, F. (2008). Asymptotically good codes. In *Advances in algebraic geometry codes*, volume 5 of *Ser. Coding Theory Cryptol.*, pages 181–220. World Sci. Publ., Hackensack, NJ.

[Özadam and Özbudak, 2009] Özadam, H. and Özbudak, F. (2009). The minimum hamming distance of cyclic codes of length $2p^s$. In Bras-Amoros, M. and Hoholdt, T., editors, *Applied Algebra, Algebraic Algorithms, And Error-Correcting Codes*, volume 5527 of *Lecture Notes in Computer Science*, pages 92–100. Springer-Verlag Berlin.

[Özadam and Özbudak, 2009] Özadam, H. and Özbudak, F. (2009). A note on negacyclic and cyclic codes of length p^s over a finite field of characteristic p. *Adv. Math. Commun.*, 3(3):265–271.

[Özbudak et al., 2009] Özbudak, E. K., Özbudak, F., and Saygı, Z. (2009). A class of authentication codes with secrecy. In *Proceedings of International Workshop on Coding and Cryptography*, pages 273–285.

[Özbudak et al., 2011] Özbudak, E. K., Özbudak, F., and Saygı, Z. (2011). A class of authentication codes with secrecy. *Des. Codes Cryptogr., to appear.*

[Özbudak and Saygi, 2006] Özbudak, F. and Saygi, Z. (2006). Some constructions of systematic authentication codes using Galois rings. *Des. Codes Cryptogr.*, 41(3):343–357.

[Sarkar and Stinson, 2001] Sarkar, P. and Stinson, D. R. (2001). Frameproof and IPP codes. In *Progress in cryptology—INDOCRYPT 2001 (Chennai)*, volume 2247 of *Lecture Notes in Comput. Sci.*, pages 117–126. Springer, Berlin.

[Sezer and Özbudak, 2008] Sezer, A. D. and Özbudak, F. (2008). Infinite families of mixed level orthogonal arrays. In *Eighth International Conference on Monte Carlo and Quasi-Monte Carlo Methods in Scientific Computing*. Canada.

[Stinson et al., 2000a] Stinson, D. R., van Trung, T., and Wei, R. (2000a). Secure frameproof codes, key distribution patterns, group testing algorithms and related structures. *J. Statist. Plann. Inference*, 86(2):595–617. Special issue in honor of Professor Ralph Stanton.

[Stinson and Wei, 2004] Stinson, D. R. and Wei, R. (2004). Generalized cover-free families. *Discrete Math.*, 279(1-3):463–477. In honour of Zhu Lie.

[Stinson et al., 2000b] Stinson, D. R., Wei, R., and Zhu, L. (2000b). New constructions for perfect hash families and related structures using combinatorial designs and codes. *J. Combin. Des.*, 8(3):189–200.

[Tang et al., 2005a] Tang, X., Udaya, P., and Fan, P. (2005a). New families of p-ary sequences from quadratic form with low correlation and large linear span. In *Sequences And Their Applications - SETA 2004*, volume 3486 of *LNCS*, pages 255–265.

[Tang et al., 2005b] Tang, X., Udaya, P., and Fan, P. (2005b). A new family of nonbinary sequences with three-level correlation property and large linear span. *IEEE Trans. Inform. Theory*, 51(8):2906–2914.

[Wang and Xing, 2001] Wang, H. and Xing, C. (2001). Explicit constructions of perfect hash families from algebraic curves over finite fields. *J. Combin. Theory Ser. A*, 93(1):112–124.

TÜBİTAK
PROJE ÖZET BİLGİ FORMU

Proje No: 107T826

Proje Başlığı:

Sonlu Cisimler ve Sonlu Halkalar Üzerinde Bazı Uygulamalar

Proje Yürütücüsü ve Araştırmacılar:

Yürütücü: Prof. Dr. Ferruh Özbudak

Araştırmacılar: Doç. Dr. Emrah Çakçak, Yard. Doç. Dr. Zülfükar Saygı

Projenin Yürütüldüğü Kuruluş ve Adresi:

ODTÜ Matematik Bölümü, İnönü Bulvarı 06531, Ankara

Destekleyen Kuruluş(ların) Adı ve Adresi:

ODTÜ Uygulamalı Matematik Enstitüsü, İnönü Bulvarı 06531, Ankara

Projenin Başlangıç ve Bitiş Tarihleri: Mart 2008 – Şubat 2011

Öz (en çok 70 kelime)

Sonlu cisimler üzerinde polinom çarpması çalışılmıştır. Daha verimli polninom çarpımı metodları geliştirilmiştir. Bulduğumuz metodlar ya olan metodlar kadar ya da onlardan da daha verimldir. Asimptotik olarak iyi parametrelere sahip lineer kodlar incelendi. Bazı çok katlı döngüsel kodların Hamming mesafeleri bulundu. Ayrıca fonksiyon cisimlerinin teorisi kullanılarak kimlik doğrulama kodları ve bu kodların güvenliği çalışıldı. Sonlu cisimler üzerinde lineer özyineleme bağıntılarının karmaşıklıkları incelendi. Çoklu dizilerin karmaşıklıkları üzerine istatiksel sonuçlar elde edildi.

Anahtar Kelimeler:

sonlu cisimler, sonlu halkalar, lineer kodlar, verimli sonlu cisim aritmetiği, kriptografi, kodlama teorisi,

Fikri Ürün Bildirim Formu **Sunuldu mu?** **Evet** **Gerekli Değil**

Fikri Ürün Bildirim Formu'nun tesliminden sonra 3 ay içerisinde patent başvurusu yapılmalıdır.

Projeden Yapılan Yayınlar:

a. [Akleylek et al.,] Akleylek, S., Cenk, M., and Özbudak, F. Faster montgomery modular multiplication without pre-computational phase for some classes of finite fields. In Proceedings of the 25th International Symposium on Computer and Information Sciences (ISCIS 2010), to appear, volume 62.

b. [Akleylek et al., 2010] Akleylek, S., Cenk, M., and Özbudak, F. (2010). Modified discrete fourier transform for efficient polynomial multiplication. In Proceedings of the 4th International Conference on Information Security and Cryptology (ISC-TURKEY 2010).

c. [Akleylek et al., 2010b] Akleylek, S., Cenk, M., and Ozbudak, F. (2010b). Polynomial multiplication over binary fields using charlier polynomial representation with low space complexity. In Proceedings of INDOCRYPT 2010, volume 6498 of Lecture Notes in Comput. Sci., pages 227–237. Springer, Berlin.

d. Akleylek et al., 2011] Akleylek, S., Cenk, M., and Ozbudak, F. (2011). On the polynomial multiplication in chebyshev form. IEEE Transactions on Computers, accepted for publication.

e. [Akleylek and Ozbudak, 2011] Akleylek, S. and Ozbudak, F. (2011). Modified redundant representation for designing arithmetic circuits with small complexity. IEEE Transactions on Computers, accepted for publication.

f. [Çalık et al., 2010] Çalık, c., Turan, M. S., and Özbudak, F. (2010). On feedback functions of maximum length nonlinear feedback shift registers. IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences, E93A(6):1226–1231.

g. , c. K., and Özbudak, F. (2009). Polynomial multiplication over finite fields using field extensions and interpolation. In Bruguera, J., Cornea, M., DasSarma, D., and Harrison, J., editors, ARITH: 2009 19TH IEEE International Symposium On Computer Arithmetic, Proceedings - Symposium on Computer Arithmetic, pages 84–91. IEEE COMPUTER SOC.

h. [Cenk and Ozbudak, 2008] Cenk, M. and Özbudak, F. (2008). Efficient multiplica-tion in F3lm , m ≥ 1 and 5 ≤ l ≤ 18. In Progress in cryptology—AFRICACRYPT 2008, volume 5023 of Lecture Notes in Comput. Sci., pages 406–414. Springer, Berlin.

i. [Cenk and Ozbudak, 2009a] Cenk, M. and Özbudak, F. (2009a). Efficient multiplication in finite fields of characteristic 3 and 5 for pairing based cryptography. In Information Security Conference.

j. [Cenk and Ozbudak, 2009b] Cenk, M. and Özbudak, F. (2009b). Improved polynomial multiplication formulas over f-2 using chinese remainder theorem. IEEE Transactions On Computers, 58(4):572–576.

k. [Cenk and Ozbudak, 2010] Cenk, M. and Özbudak, F. (2010). On multiplication in finite fields. J. Complexity, 26(2):172–186.

l. [Fu et al., 2009] Fu, F.-W., Niederreiter, H., and Özbudak, F. (2009). Joint linear complexity of arbitrary multisequences consisting of linear recurring sequences. Finite Fields Appl., 15(4):475–496.

m. [Guneri and Ozbudak, 2008] Güneri, C. and Özbudak, F. (2008). Weil-Serre type bounds for cyclic codes. IEEE Trans. Inform. Theory, 54(12):5381–5395.

n. [Kaskaloglu and Ozbudak, 2010] Kaskaloglu, K. and Özbudak, F. (2010). On hierarchical threshold access structures. In Proceedings of Information Systems Technology Panel Symposium, IST-091/RSY-021.

o. [Koyuncu and Ozbudak, 2009] Koyuncu, F. and Özbudak, F. (2009). Integral and homothetic indecomposability with applications to irreducibility of polynomials. Turkish J. Math., 33(3):283–294.

p. [Koyuncu and Ozbudak, 2011] Koyuncu, F. and Ozbudak, F. (2011) Probabilities for absolute irreducibility of multivariate polynomials by the polytope method. Turkish Journal of Mathematics, accepted for publication.

q. [Meidl and Ozbudak, 2008] Meidl, W. and Özbudak, F. (2008). Generalized joint linear complexity of linear recurring multisequences. In Sequences and their applications—SETA 2008, volume 5203 of Lecture Notes in Comput. Sci., pages 266–277. Springer, Berlin.

r. [Meidl and Ozbudak, 2009] Meidl, W. and Özbudak, F. (2009). Linear complexity over Fq and over Fqm for linear recurring sequences. Finite Fields Appl., 15(1):110–124.

s. [Niederreiter and Ozbudak, 2008] Niederreiter, H. and Özbudak, F. (2008). Asymp-totically good codes. In Advances in algebraic geometry codes, volume 5 of Ser. Coding Theory Cryptol., pages 181–220. World Sci. Publ., Hackensack, NJ.

t. [Ozadam and Ozbudak, 2009] Özadam, H. and Özbudak, F. (2009). The minimum hamming distance of cyclic codes of length 2p . In Bras-Amoros, M. and Hoholdt, T., editors, Applied Algebra, Algebraic Algorithms, And Error-Correcting Codes, volume 5527 of Lecture Notes in Computer Science, pages 92–100. Springer-Verlag Berlin.

u. [Ozadam and Ozbudak, 2009] Özadam, H. and Özbudak, F. (2009). A note on negacyclic and cyclic codes of length p over a finite field of characteristic p. Adv. Math. Commun., 3(3):265–271.

v. [Ozbudak et al., 2009] Özbudak, E. K., Özbudak, F., and Saygı, Z. (2009). A class of authentication codes with secrecy. In Proceedings of International Workshop on Coding and Cryptography, pages 273–285.

w. [Ozbudak et al., 2011] Ozbudak, E. K., Ozbudak, F., and Saygı, Z. (2011). A class of authentication codes with secrecy. Des. Codes Cryptogr., to appear.

x. [Sezer and Ozbudak, 2008] Sezer, A. D. and Özbudak, F. (2008). Infinite families of mixed level orthogonal arrays. In Eighth International Conference on Monte Carlo and Quasi-Monte Carlo Methods in Scientific Computing. Canada.