HACETTEPE ÜNİVERSİTESİ • MATEMATİK BÖLÜMÜ

LİSANSÜSTÜ SEMİNERLERİ IV

• PROGRAM •

21 Mayıs 2025, Çarşamba

Hacettepe Üniversitesi • Matematik Bölümü • Yaşar Ataman Toplantı Salonu

10:00 – 10:30

AHSEN SENA YURTOĞLU
Lokal Solid Vektör Latisleri Üzerinde Tanımlanan Bazı Operatör Sınıfları

10:40 – 11:10

SERGEN AYYILDIZ
Kuasi-Kompakt C_0-Yarıgruplarının Düzgün Ortalama Ergodikliğinin İncelenmesi

11:20 – 11:50

EGEMEN ÇEKEN
Invariant Random Subgroups

12:00 – 13:30

ARA

13:30 – 14:00

BARIŞ SURFACI
Klasik Kriptografiden Kuantum-Sonrası Kriptografiye

14:10 – 14:40

MUSTAFA SOLMAZ
Çok Değişkenli Polinom Tabanlı Kriptografi Üzerine

14:50 – 15:20

EMRE CAN ERDEM
Düğüm Teorisi ve Uygulamaları

Lokal Solid Vektör Latisleri Üzerinde Tanımlanan Bazı Operatör Sınıfları

Ahsen Sena Yurtoğlu

Bursa Teknik Üniversitesi, Mühendislik ve Doğa Bilimleri Fakültesi, Matematik Bölümü, Bursa, Türkiye

Özet

Son yıllarda Banach latisleri üzerindeki operatör sınıfları kapsamlı biçimde incelenmiş olsa da, lokal solid vektör latisleri üzerindeki çalışmalar daha zengin bir yapının anlaşılmasını sağlamaktadır. Lokal solid vektör latisleri, hem sıralı yapı hem de topolojik yapı içerdiğinden, operatör davranışları Banach latislerinden farklılık gösterebilmektedir.

1966'da tanımlanan demisürekli ve demikompakt operatörler, sabit nokta kuramına katkı sağlamış ve Banach latislerinde çeşitli genellemeleri detaylı biçimde çalışılmıştır. Bu çalışma, lokal solid vektör latisleri üzerinde tanımlanan quasi KB ve demi quasi KB operatörlerinin temel özelliklerini ele almakta ve aralarındaki ilişkileri incelemektedir. Bu çalışma, Doç. Dr. Nazife Erkurşun Özcan ile birlikte yürütülmüş ortak bir çalışmadır.

Kuasi-Kompakt C_0-Yarıgruplarının Düzgün Ortalama Ergodikliğinin İncelenmesi

Sergen Ayyıldız

Ankara Üniversitesi, Fen Fakültesi, Matematik Bölümü, Fonksiyonel Analiz Anabilim Dalı
Hacettepe Üniversitesi, Fen Fakültesi, Matematik Bölümü

Özet

Banach uzayı üzerinde tanımlı operatörlerin oluşturduğu güçlü sürekli yarıgrupların teorisi birçok alanda uygulaması bulunan aktif bir teoridir. X Banach uzayı olmak üzere $\left(T(t)\right)_{t\geq 0}$ operatör ailesine $T(0)=I, T(t+s)=T(t)T(s)$ ve her $x\in X$ için $lim_{t\downarrow 0}T(t)x=x$ koşullarını sağlıyor ise güçlü sürekli tek parametreli operatör yarıgrubu veya kısaca C_0-yarıgrubu adı verilir.

Bu konuşmada öncelikle C_0-yarıgrubu örnekleri verilecek, bir C_0-yarıgrubunun üreteci ve özellikleri ile kapalı ve yoğun tanımlı üretecin ürettiği $\left(T(t)\right)_{t\geq 0}$ C_0-yarıgrubunun biricikliğine değinilecektir. Daha sonra bir C_0-yarıgrubunun kuasi-kompakt olma koşulları tartışılacaktır. Ayrıca kuasi-kompakt C_0-yarıgrubunun düzgün ortalama ergodik olduğunun kanıtı verilecektir. Bu konuşma, Doç. Dr. Nazife Erkurşun Özcan ile birlikte yürütülen yüksek lisans tezi ile bağlantılıdır.

Invariant Random Subgroups

Egemen Çeken

Hacettepe University

Abstract

An Invariant Random Subgroup (IRS) of a countable group Γ is a Borel probability measure on the space of subgroups of Γ, denoted Sub_Γ, which is invariant under the conjugation action of Γ. This concept captures the idea of selecting a subgroup at random in a way that is consistent with the group's conjugation action. IRSs generalize constructions such as normal subgroups and conjugacy classes, and offer a probabilistic framework for studying subgroup structure.

This seminar focuses on a special class of IRSs known as diffuse IRSs, which are ergodic and assign measure zero to every isomorphism class of subgroups. In such cases, a randomly chosen subgroup is almost surely not isomorphic to any fixed group. These measures reflect a high degree of randomness and stand in contrast to classical IRSs, which often concentrate on a single isomorphism type.

After introducing background on measure theory, hyperbolic geometry, and the Chabauty topology, the talk discusses ergodic and diffuse IRSs and how the ergodic decomposition theorem helps classify them. The central question is whether diffuse IRSs actually occur in nature—and if so, how to construct them.

Two constructions are presented. The first uses a semidirect product $H = N \rtimes \Gamma$ where a conjugation-equivariant map lifts an ergodic IRS on Γ to a diffuse IRS on H. The second involves hyperbolic reflection groups and Coxeter polygons. By controlling the angle sequences in a family of tilings of the hyperbolic plane, one obtains a limit IRS with support on uncountably many non-isomorphic subgroups. This leads to the $*$-property, which guarantees such structural richness.

These results confirm that diffuse IRSs do exist and can be explicitly constructed in both algebraic and geometric settings. They highlight the diversity of subgroup behavior and offer new perspectives in the probabilistic study of groups.

Klasik Kriptografiden Kuantum-Sonrası Kriptografiye

Barış Surfacı

Özet

Gelişen teknoloji ile birlikte kuantum bilgisayarlar gündeme gelmiştir. Kuantum bilgisayarları klasik bilgisayarlardan ayıran en belirgin özellik, işlem hızlarının çok daha yüksek olmasıdır. Bunun sebebi, günümüz bilgisayarlarının işlem yaparken transistörleri kullanmasıdır. Transistörler sadece iki gerilim seviyesine sahiptirler. Bu seviyeler, neredeyse herkesin bir yerlerden duymuş olduğu "0" ve "1"lerdir. Klasik bilgisayar dilinde bu sayılar bit olarak adlandırılır ve bir klasik bilgisayarda bitler aynı anda sıfır ve bir olamazlar. Kuantum bilgisayarlarda ise bitler "süperpozisyon" adı verilen ve anlamca karşılığı "hem sıfır hem bir olma durumu" olan bir halde bulunabilirler. Bu sayede bir kuantum bilgisayar aynı anda birden fazla biti okuyabilir. Kuantum hesaplamayla uğraşan bilim insanları, kuantum bitleri normal bitlerden ayırmak için kuantum-bit anlamına gelen "kübit" terimini kullanmaktadırlar. Kısacası, bir klasik bilgisayar aynı anda bir bitlik işlem yaparken, bir kuantum bilgisayar bir kübitlik, yani iki bitlik, işlem yapabilmektedir. Ayrıca, iki kübitin yan yana gelme durumu 4 bit değerinde olurken, 3 kübitin yan yana gelme durumu 8 bitlik bir veri değeri oluşturmaktadır; benzer şekilde devam edildiğinde n tane kübitin yan yana gelme durumu da 2^n bitlik veri okuma değeri ortaya çıkarıyor. Dolayısıyla, aynı zaman aralığında bir klasik bilgisayarın okuduğu veri miktarının, bir kuantum bilgisayar üstel olarak katlanmış kadarını okuyabiliyor. Bu da, kuantum bilgisayarların klasik bilgisayarlardan neden çok daha hızlı olduğunu açıklıyor.

Klasik kriptosistemler bit dizgeleri üzerinden işlemektedir. Bit dizgeleri, belirli bir sayıda bitin yan yana sıralanarak oluşturduğu kelimeler olarak görülebilir. Bir klasik şifreleme sistemini kırmak için de bu dizgelerden bazılarını biliyor olmak yeterlidir. Fakat algoritma içerisinde gizli tutulan bir dizgenin bulunabilmesi için çok fazla sayıda deneme yapmak gerekebilir. Klasik bilgisayarlarla bu denemeleri yapmak milyar yıllar sürebilirken, bir kuantum bilgisayar için bu süre, ilk paragrafta açıkladığımız sebepten ötürü, çok daha kısa sürmektedir. Dolayısıyla, kuantum bilgisayarların hayatımıza girmesiyle birlikte, klasik kriptosistemlerin sağladığı güvenlik durumu tehlikeye düşmektedir. Bu sebeple, kuantum bilgisayarlara bile direnebilecek yeni algoritmalara ihtiyaç duyulmuştur. Bu algoritmalar için kullanılan dizgelerin matematik dilindeki karşılığını, bir sayının yerine bir polinom yazmak olarak görebiliriz. Bir sayının yerine kullanılan polinomu t dereceli kabul edersek, algoritmayı kırmak için bir tek sayıyı bulmak yerine, t tane sayı bulmamız gerektiği anlamına gelir. Bu da kuantum bilgisayarları bile fazlasıyla oyalayacak demektir.

Kuantum-sonrası kriptografik algoritmalar 4 ana başlık altında toplanmıştır: kod tabanlı, kafes tabanlı, çok değişkenli polinom tabanlı ve özet tabanlı. Bu dört temel kategoriden en dayanıklı olanı kafes tabanlılardır. Çünkü kafes tabanlı algoritmaların temelinde yatan matematiksel problemler çok daha fazla deneme sayısı gerektirir ve bu durum, kuantum bilgisayarları bile yüksek derecede zorlayan bir durumdur.

Çok Değişkenli Polinom Tabanlı Kriptografi Üzerine

Mustafa Solmaz

Hacettepe Üniversitesi

Özet

Kriptografi güvenli kriptosistemler kurabilmek için çeşitli matematiksel zorluklardan yararlanır. Açık anahtar kriptografisi dijital imzalama ve anahtar paylaşımı için kullandığımız bir kriptografik yöntemdir. Shor'un kuantum algoritması (1994) gibi bazı algoritmalar, günümüz açık anahtar kriptosistemlerinin dayandığı asal çarpanlara ayırma problemi, ayrık logaritma problemi v.s. gibi klasik bilgisayarlarda üstel zamanda çözülebilecek problemlerin kuantum hesaplama gücüne sahip cihazlarda polinom zamanda çözebileceğini göstermiştir. Bu tür bir tehdide karşılık olarak kriptografi dünyası gelecekteki olası kuantum cihazlarının kullanımına karşı güvenli kriptosistemler kurabilmek için farklı matematiksel zorluklardan yararlanmayı amaçlamaktadır. Bu matematiksel zorluklardan en önemlilerinden biri olan MQ-Problem (Multivariate Quadratic), ikinci dereceden çok değişkenli katsayıları bir sonlu cisimden gelen polinom sistemindeki tüm polinomlar için ortak bir kök bulma problemidir. Bu problemin karar aşamasının bile NP-tam bir problem olduğu ispatlanmıştır (1979, M.R. Garey, D.S. Johnson). Çok değişkenli polinom tabanlı kriptografi güvenlik iddiasını MQ-Probleme dayandıran, kriptografik operasyonlarını çok değişkenli polinomlar üzerinde gerçekleştiren kriptosistemlerin genel adı olarak tanımlanabilir. En eski çok değişkenli polinom tabanlı kriptosistemlerinden biri olan Matsumoto-Imai kriptosistemi (1988), Jacques Patarin tarafından bir lineerleştirme atağıyla 1995 yılında kırılmış olmasına karşın güncellenerek sonrasında çıkan HFE (Hidden Field Equations) ve diğer HFE varyantlarına ilham olmuştur. Daha sonra 1999 yılında Patarin, Kipnis, Shamir tarafından yayınlanan UOV (Unbalanced Oil and Vinegar) şeması, polinomlarının özel kurulumlarından ötürü imzalama işlemini Gauss eliminasyonu gibi çok temel lineer cebir işlemleriyle yaparak verimli ve hızlı çalışma özelliğine sahiptir. Çeyrek asırı aşan geçmişine rağmen günümüzde hala birçok farklı varyantıyla birlikte araştırılmaya devam edilmektedir. Bu sunumda öncelikle çok değişkenli polinom tabanlı kriptografinin ortaya çıkışı, altında yatan cebirsel yapılar, ilk şemalar tanıtılacaktır. Bu tür şemaların tarihsel gelişimiyle birlikte üzerinde araştırılmaya ihtiyaç du-yulan NIST'in 2017–2022 yılları arasında gerçekleştirdiği Kuantum Sonrası Dijital İmzalama Standartizasyonu yarışmasında üçüncü tur finalistlerinden Rainbow, 2023 yılında duyurduğu 2025 yılı itiba-riyle devam etmekte olan yeni standartlar belirlemeyi amaçlayan Kuantum Sonrası Dijital İmzalama yarışmasına devam eden UOV ve MAYO gibi önde gelen çok değişkenli polinom tabanlı projelerden bahsedilecektir.

Düğüm Teorisi ve Uygulamaları

Emre Can Erdem

Özet

Üç boyutlu manifoldlar içerisinde kendi kendisini kesmeyen kapalı eğrilere düğüm adı verilmektedir. Düğüm teorisi, biyoloji, kimya ve fizik gibi çeşitli bilimsel alanlarda geniş uygulama alanı bulan, zengin ve dinamik bir çalışma konusudur. Bu tez kapsamında, düğüm teorisinin temel kavramları, düğümlerin geometrik ve topolojik özellikleri ile düğüm değişmezleri sistematik olarak incelenmiştir. Ayrıca, düğüm teorisinin farklı bilim alanlarından Veri Analizi, Fizik, Robotik, Biyoloji ve Geometrik Topoloji alanlarındaki uygulamalarına ilişkin güncel araştırmalar derlenmiş ve ayrıntılı şekilde ele alınmıştır.