第７回組合せ論若手研究集会
招待講演アブストラクト

平成23年2月21日（月）～ 2月23日（水）
慶應義塾大学矢上キャンパス
14棟想創館2階14-203番教室（セミナールーム３）

2月21日（月）　新國亮氏（東京女子大学）

「Conway-Gordonの定理とその周辺」

グラフを自然に位相空間とみなして3次元Euclid空間に埋め込んだものを空間グラフという. 特にグラフがサイクル(の非交和)に同相であるとき, その空間グラフは結び目(絡み目)と呼ばれる. 空間グラフ理論とは, 空間グラフをトポロジー, 特に結び目理論の立場から研究する分野である. 本講演では, 空間グラフ理論において最も有名な定理であるConway-Gordonの定理及びその周辺の話題を取り上げ, 近年得られた結果を紹介する.

2月22日（火）　平井広志氏（東京大学）

「重み付き多品種流最大化問題」

有限集合Sを頂点部分集合(ターミナル)としてもつ無向グラフGの多品種流(フロー)とは、Sの異なる点を結ぶパス(S-パス)の集合とその上の非負流量値関数であって容量条件—各枝の流量の総和が1以下—を満たすものとする．今、Sのペア上の非負値関数μが与えられていて、パスがペア$\{s,t\}$を結ぶとき，その1フロー毎の価値を$\mu(s,t)$とする．μ重み付き多品種流最大化問題とは、多品種流であって価値の総和を最大化するものを求める問題である．

例えば、Sを4点集合$\{s,t,s',t'\}$，μをペア$\{s,t\}$,$\{s',t'\}$上で1，それ以外で0と定義すれば2品種流問題となり、半整数値の最大フローが存在する(Hu 63)．一方、フローを整数値に制限するとNP困難となる(Even-Itai-Shamir 76)．Sを一般の有限集合で、μをすべてのペアで1とするとS-パス詰込み問題となり、この場合も半整数値の最大フローが存在する(Lovasz 76, Cherkassky 77) 実は、フローを整数値に制限しても最大最小型定理が

成立することが知られており(Mader 78)，さらに線形マトロイドマッチングへの帰着によって多項式時間可解となる(Lovasz 80, Schrijver 03).

さて、以上の観察に基づいて、次の分類問題を考える：

1. ある正整数kが存在して、すべてのグラフに対して$1/k$-整数最大フローが存在する重みμは何か？そしてkが取り得る値は何か？
2. フローを整数値に制限しても、多項式時間可解となる重みμは何か？
3. この分類問題はA. Karzanovによって70年代から90年代にいたるまで、主に0-1値重みに対し考察されてきた．講演では、この問題に対する数理と最近の結果について紹介したい.

2月23日（水）　萩田真理子氏（お茶の水女子大学）

「有限体の暗号アルゴリズムへの応用」

コンピュータとインターネットを基盤とした今のウェブ社会では暗号に代表される情報セキュリティアルゴリズムの役割が大きくなっていますが，これらのアルゴリズムには，実は離散数学が大きく貢献しています。特に有限体についての知識があれば，どういう意図でそれぞれのアルゴリズムが作られたのか, 理解しやすくなっています。

前半は，整数環と有限体について暗号などのアルゴリズムで扱いやすい形で解説し，後半では, 素数判定アルゴリズム, 擬似乱数, 暗号への具体的な応用例を紹介します。特に擬似乱数と暗号乱数のアルゴリズムのどの部分が周期に影響しているか，それぞれの関数がどのような目的で構成されているか解説する予定です。