

Juan González-Meneses (Universidad de Sevilla)

Trenzas: de los automorfismos de superficies a la criptografía

Las trenzas son unos objetos topológicos muy relacionados con los nudos o con los automorfismos de superficies. Actualmente el estudio de las trenzas está experimentando un auge importante, debido a sus posibles aplicaciones a la criptografía. En concreto, la dificultad del problema de conjugación en los grupos de trenzas es la pieza clave de los criptosistemas propuestos.

Pero no está tan claro que el problema de la conjugación en estos grupos sea suficientemente difícil, desde el punto de vista computacional, ya que hay muchas herramientas disponibles para estudiar las trenzas. En esta charla veremos cómo la teoría de Nielsen-Thurston de automorfismos de superficies, aplicada a los grupos de trenzas, produce resultados puramente algebraicos que podrían conducir a la resolución del problema de la conjugación en tiempo polinomial.