Curs 2010-2011

Títol: Grups de trenes

Objectius:

Demostrar que tot nus és la clausura d'alguna trena. Conèixer els grups de trenes i algunes de les seves representacions. Discutir el problema de les paraules i el problema de la conjugació. Introduir les tècniques de criptografia basada en grups de trenes.

Temari:

1. Conceptes bàsics sobre nusos

1.1. Isotopies a l'espai tridimensional
1.2. Teorema de Reidemeister
1.3. Superfícies de Seifert

2. Trenes

2.1. Grups d'Artin
2.2. Algorisme de Yamada-Vogel
2.3. Teorema de Markov

3. Criptografia basada en grups

3.1. Introducció a la teoria combinatòria de grups
3.2. Complexitat algorísmica del problema de la conjugació
3.3. Tècniques de criptografia amb grups de trenes

Bibliografia:

Adams, C. C., *The Knot Book: An Elementary Introduction to the Mathematical Theory of Knots*, W. H. Freeman and Company, New York, 1994.

Birman, J. S., Brendle, T. E., Braids: a survey, *Handbook of Knot Theory*, Elsevier, Amsterdam, 2005, 19–103.

Burde, G., Zieschang, H., *Knots*, de Gruyter, Berlin (1a ed. 1985, 2a ed. 2003).

Cromwell, P. R., *Knots and Links*, Cambridge University Press, Cambridge, 2004.

Franco, N., González-Meneses, J., Conjugacy problem for braid groups and Garside groups, *J. Algebra* **255** (2003), 112–132.

Magnus, W., Karrass, A., Solitar, D., *Combinatorial Group Theory: Presentations of Groups in Terms of Generators and Relations*, Dover, New York, 2004 (1a ed. Wiley Interscience, New York, 1966).