**Mercoledì 2 Marzo 2022 – ore 16:00**

**Seminario Online via Zoom**

***Seminario congiunto UMI - Gruppo Crittografia e Codici e Iniziativa De Componendis Cifris - Gruppo MathCifris***

***Martino Borello***

**Université Paris 8-LAGA**

**Il principio di indeterminazione dal punto di vista della teoria dei codici**

**Abstract:**  Il principio di indeterminazione è un risultato classico dell'analisi armonica che afferma che, data una funzione non nulla f su un gruppo abeliano, almeno una tra *f* e la sua trasformata di Fourier hanno un supporto grande (si veda per esempio [4]).

In [3], gli autori mostrano come questo principio, considerato su campi finiti, è strettamente legato al problema dell'esistenza di codici ciclici asintoticamente buoni, cioè ideali dell'algebra di gruppo *KCn* (dove *Cn* è un gruppo ciclico di ordine *n*) la cui dimensione su *K* e la distanza minima (di Hamming) sono funzioni lineari in *n*. Tale problema è considerato come uno dei più importanti problemi aperti nella teoria classica dei codici [1]. Nel seminario, presenteremo questi due problemi e la loro connessione, e poi discuteremo gli sviluppi più recenti (vedi [2]) e le prospettive future di ricerca.

[1] E. Assmus, H. Mattson, and R. Turyn. Cyclic codes, af cambridge research labs, bedford. Technical report, AFCRL-66-348, 1966.

[2] M. Borello and P. Solé. The uncertainty principle over finite fields. Discrete Mathematics, 345(1):112670, 2022.

[3] S. Evra, E. Kowalski, and A. Lubotzky. Good cyclic codes and the uncertainty principle. L’Enseignement Mathématique, 63(3):305–332, 2018.

[4] T. Tao. An uncertainty principle for cyclic groups of prime order. Mathematical Research Letters, 12(1):121–127, 2005.

[**Link al seminario su Zoom**](https://unitn.zoom.us/j/81899507212)

ID riunione: 818 9950 7212

Passcode: 437101