



OP	a	b	c	d	e	f	g	h	i	l	m
	x	y	z	n	o	p	q	r	s	t	u
QR	a	b	c	d	e	f	g	h	i	l	m
	q	r	s	t	u	x	y	z	n	o	p
ST	a	b	c	d	e	f	g	h	i	l	m
	p	q	r	s	t	u	x	y	z	n	o
VX	a	b	c	d	e	f	g	h	i	l	m
	u	x	y	z	n	o	p	q	r	s	t
YZ	a	b	c	d	e	f	g	h	i	l	m
	o	p	q	r	s	t	u	x	y	z	n



Mercoledì 6 Ottobre 2021 – ore 16:00

Seminario Online via Zoom

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

Alessandro Neri

Max Planck Institute for Mathematics in the Sciences, Lipsia

Matrici Parziali e Polinomi non Commutativi nella Teoria dei Codici

Abstract: La teoria algebrica dei codici può essere vista come la teoria dei sottospazi di un dato spazio metrico. Il caso più studiato è senza dubbio quello dei codici con la metrica di Hamming. In questa situazione, viene considerato un spazio vettoriale finito-dimensionale su un campo (finito) K , dove la distanza tra due vettori è data dal numero di entrate in cui essi differiscono. Negli ultimi decenni, l'attenzione di molti ricercatori si è spostata sui codici con la metrica del rango, ovvero sottospazi di matrici a coefficienti in un campo K , in cui la distanza tra due matrici è il rango della loro differenza. Recentemente, una nuova metrica è diventata molto popolare: la metrica sum-rank. Lo spazio ambiente è fatto da tuple di matrici, e la distanza tra due tuple è misurata sommando i ranghi delle differenze delle rispettive matrici. Tuttavia, questi spazi metrici possono essere visti come casi particolari di un setting molto più generale, ovvero spazi di matrici in cui alcune entrate sono fissate uguali a zero.

In questo talk inizierò dando una prima overview storica su problemi e risultati analoghi trattati in letteratura, in diversi ambiti di ricerca. In seguito, presenterò un framework unificato che racchiude i diversi spazi metrici. In particolare, mostrerò come, sotto certe ipotesi sul campo di definizione, questi spazi metrici sono isometrici a dei particolari anelli di polinomi non commutativi. Infine, usando queste isometrie, costruirò spazi di matrici a blocchi in cui tutte le matrici non nulle hanno rango alto. Come conseguenza di queste costruzioni, si ottiene una nuova famiglia di codici MDS additivi nella metrica di Hamming.

[Link al seminario su Zoom](#)

ID riunione: 859 2315 4700

Passcode: 101986

Referente

Norberto Gavioli

Associazione De Componendis Cifris

seminari@decifris.it
segreteria@decifris.it
matematica@decifris.it

UMI

seminariumi-cc@googlegroups.com