DIPARTIMENTO DI
INFORMATICA, SISTEMISTICA E
COMUNICAZIONE

Viale Sarca, 336
20126 Milano

SEMINAR ANNOUNCEMENT

Thursday September 1st, 2022

03:00 pm
Seminar Room, first floor, Abacus Building (U14)
Department of Informatics, Systems and Communication

Counting coprime polynomials... with complications

Speakers:

Luca Mariot, Radboud University, the Netherlands

Abstract:

The construction of coprime polynomials over finite fields has several applications in cryptography, coding theory and combinatorics. In the binary field GF(2), Benjamin and Bennett showed a simple way to count and enumerate coprime polynomial pairs based on what they call DilcuE’s algorithm (i.e., Euclid’s algorithm ran backwards). In this talk, we consider a specific case of the above problem, namely when both polynomials have the same degree and a nonzero constant term, which is motivated by the design of secret sharing schemes via cellular automata. Interestingly, this variant turns out to be more complicated, requiring different approaches ranging from formal languages to combinatorics to solve different aspects of the problem. In particular, we decompose our problem in two parts. First, we show that the sequences of constant terms for the quotients visited by DilcuE's algorithm can be modeled as words of a regular language recognized by a simple finite state automaton. This allows us in turn to count all such sequences by leveraging on classic results from algebraic language theory. On the other hand, we show that the sequences of degrees of quotients in DilcuE's algorithms are equivalent to compositions of natural numbers, which have a simple description in terms of partially ordered sets. Putting these two results together, we finally devise a combinatorial algorithm that enumerates all pairs of coprime polynomials with nonzero constant term of given degree.

Biographies:

Luca Mariot, is currently a postdoc researcher in the Digital Security Group at Radboud University in Nijmegen, the Netherlands. His main research interests lie at the intersection of cryptography and artificial intelligence, focusing on computational models such as cellular automata and bio-inspired optimization techniques such as evolutionary algorithms to design cryptographic primitives. Previously, Luca was a postdoc in the Cyber Security Research Group at TU Delft, the Netherlands, and at the University of Milano-Bicocca, Italy. He received his PhD in Computer Science in 2018 under a double degree agreement, from the University of Milano-Bicocca and the Université Côte d'Azur, France.

Contact person for this Seminar: Alberto Leporati