ID de Contribution: **7** Type: **Non spécifié**

On shuffles and permutations

vendredi 28 novembre 2025 09:00 (50 minutes)

Shuffle permutations appear in many different contexts, such as Hopf algebras, shift registers in coding theory and kryptology, symbolic dynamics for chaotic dynamical systems, card tricks, and in the design of efficient permutation networks for parallel computing.

I will give a leisurely discussion of shuffles in various contexts, and in particular discuss the problem of designing interconnection networks for massively parallel computers.

The classical Shuffle-Exchange (SE) network is built around the basic operations of card shuffling and bipartite Exchange swaps. SE networks can perform any permutation of n items in $2\log_2(n)$ steps, with only $3n$ interconnection wires, yielding an optimal 'cost' $c = 6n\log_2(n)$. SE networks are, however, difficult to construct due to their complicated non-recursive structure.

A class of generalised Shuffle-Exchange (GSE) networks is introduced. As permutation networks these have the same functionality as SE, but some of them possess recursive structures lacking in the classical SE net. This makes them possibly very attractive from a hardware-designers point of view.

Based on the theory of linear recurrences over Galois Fields and linear shift registers, we develop the theory of GSE networks and present general theorems showing how to construct such networks built up recursively by using identical (or a small number of different) building blocks.

Orateur: MUNTHE-KAAS, Hans (University of Bergen)