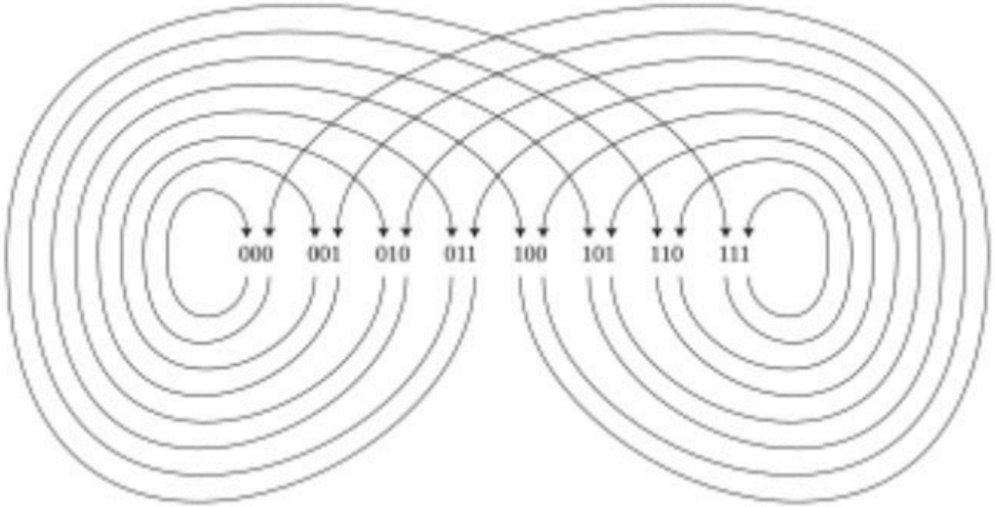
On Permutations and Shuffles

Celebrating Dominique Manchon, Clermont-Ferrand 2025

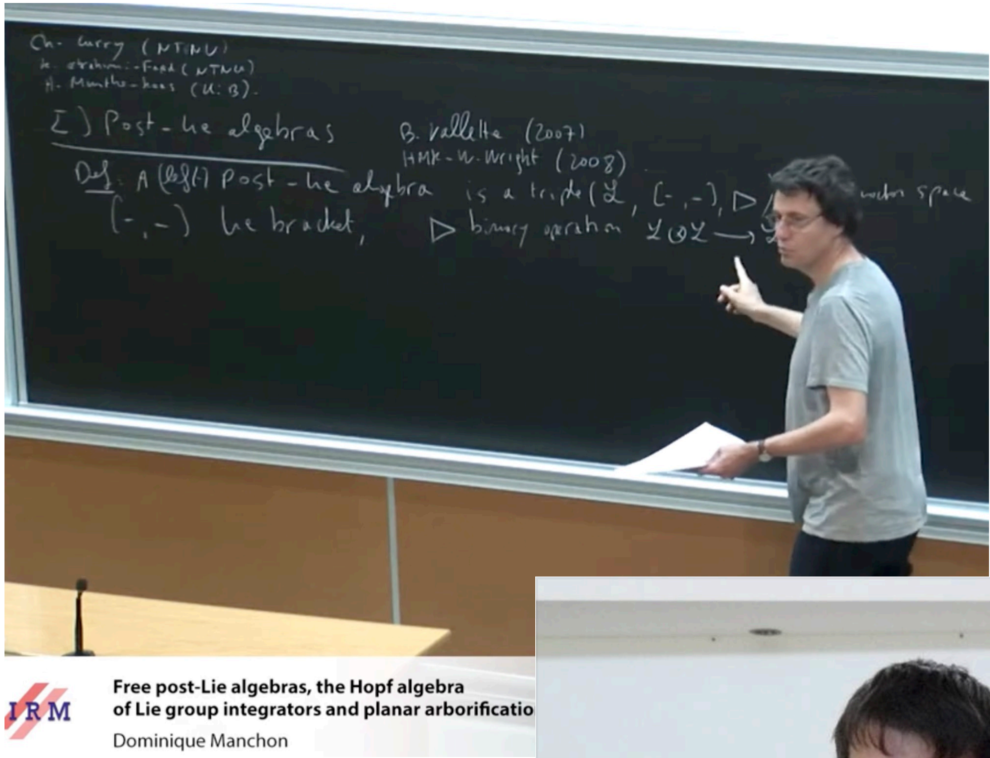
Hans Munthe-Kaas
Lie Størmer Center
UIT The Arctic University of Norway
UIB University of Bergen
hans.munthe-kaas@uit.no
hans.munthe-kaas.no



Binary De Bruijn graph

Lorenz attractor

Dominique


IRM
Free post-Lie algebras, the Hopf algebra
of Lie group integrators and planar arborificatio
Dominique Manchon

Max-Planck-Institut für Mathematik, Bonn

Conference on

COMBINATORICS AND PHYSICS

Matilde Marcolli
Walter D. van Suijlekom
Kurusch Ebrahimi-Fard

March 19-23, 2007

Lecturers:

Pierre Cartier
Philippe Di Francesco
Predrag Cvitanoviœ
Frédéric Patras

Speakers:

Christian Brouder
Alain Connes
Loïc Foissy
Arieh Iserles
Dirk Kreimer
Dominique Manchon
Ângela Mestre
Daniele Oriti
Christophe Tollu
Paul Zinn-Justin
Francis Brown
Gérard H.E. Duchamp
Massimiliano Gubinelli
Thomas Krajewski
Jean-Louis Loday
Fotini Markopoulou Kalamara *
Hans Munthe-Kaas
Sylvie Paycha
Xavier Viennot
Don Zagier

* to be confirmed

Further information:

E-Mail: combphys07@mpim-bonn.mpg.de
WWW: http://www.mpim-bonn.mpg.de/Events/This+Year+and+Prospect/

Our first meeting
Bonn 2007

Shuffles

Out-shuffle: n -> (2 n) % 51

0 1 2 3 ... 25 26 27 28 ... 50 51 ⟶ 0 26 1 27 2 28 3 ... 50 25 51

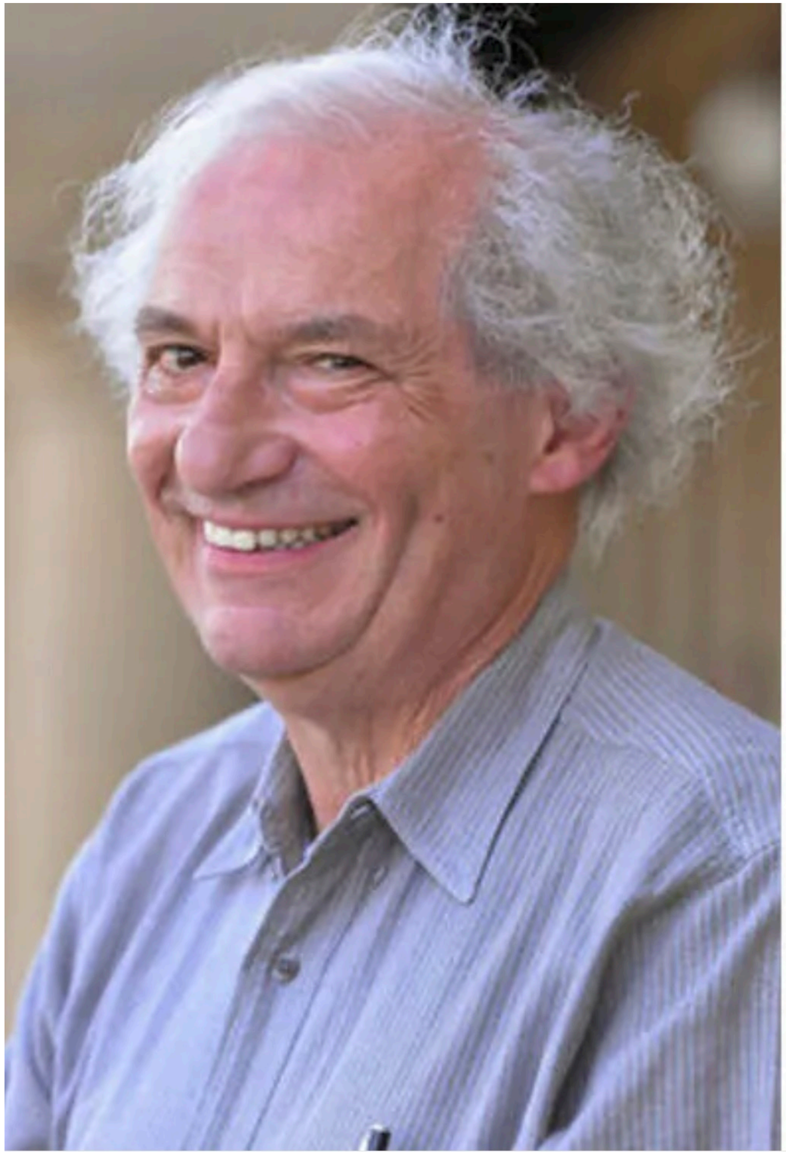
In-shuffle: n -> (2 n+1) % 53

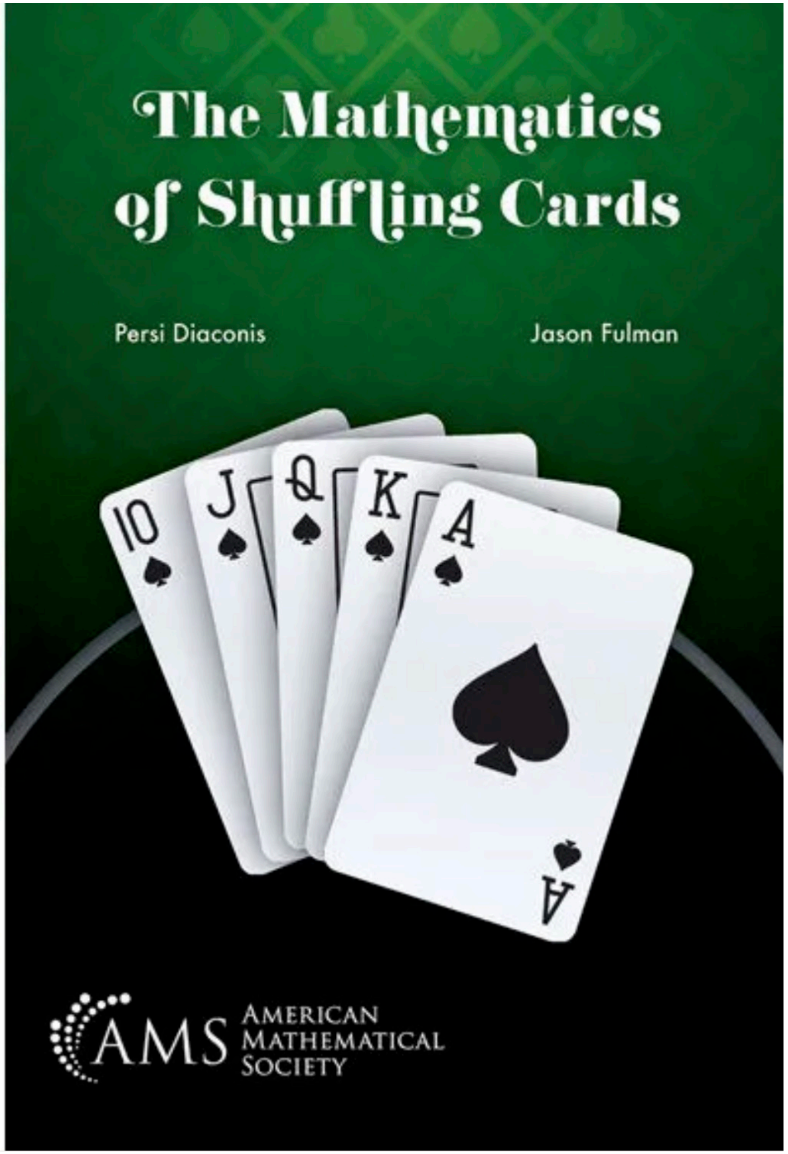
0 1 2 3 ... 25 26 27 28 ... 50 51 ⟶ 26 0 27 1 28 2 ... 50 24 51 25

- Steve Smale, Rufus Bowen:
  Horseshoe map, Axiom A flows, Markov partitions
- Solomon Golomb, E. Selmer:
  Shift registers
- Persi Diaconis:
  Card tricks, statistics
- Eilenberg MacLane:
  Shuffle Hopf algebra

Persi Diaconis

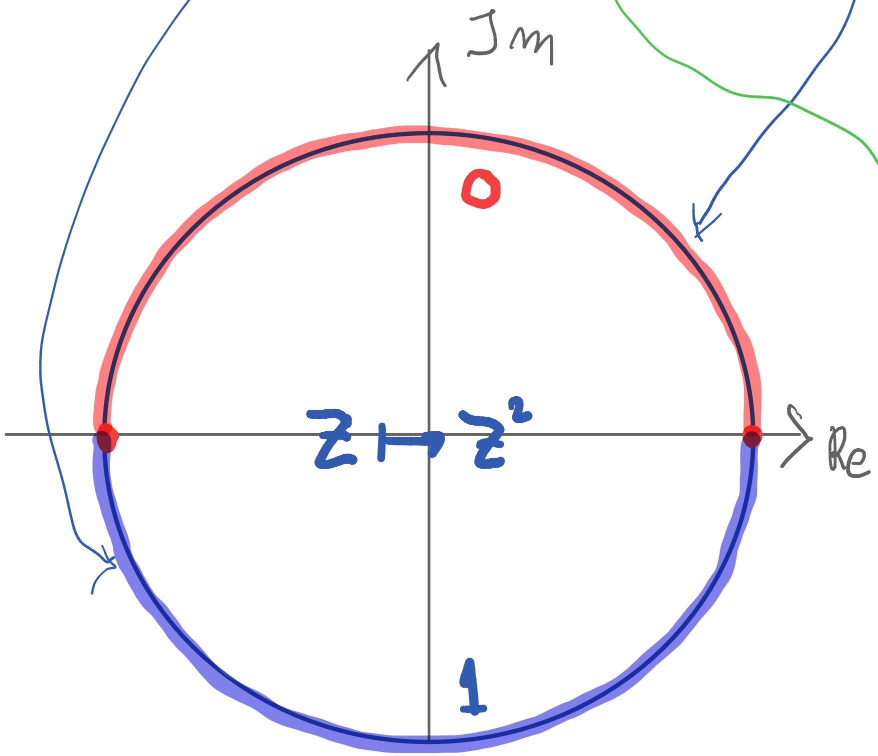
sleight-of-hand artist, mathematician, statistician





Continuous shuffles and dynamical systems

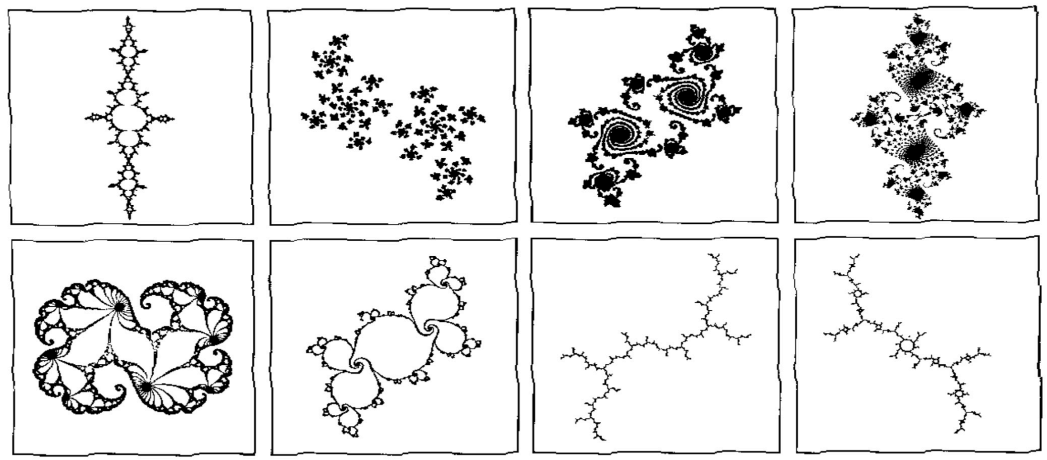
Chaotic dynamics, Markov partitions and symbolic dynamics



$$z = e^{2\pi i \theta}, \quad \theta \longmapsto 2\theta \ (\mathrm{mod}\ 1)$$

θ : 0100111010100011 ....

Julia Sets



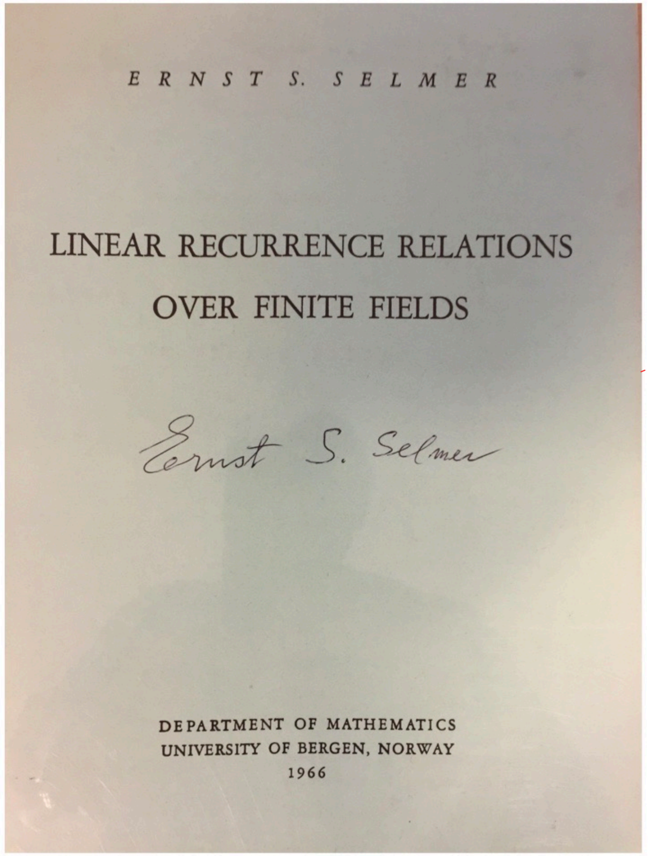
Shuffles are universally present in mixing flows and chaotic dynamics

Entropy : $H = -\sum_i p_i \log p_i$

Shannon 1948, Kolmogorov-Sinai 1958, Rufus Bowen, Steve Smale, ...

Ernst S. Selmer (1920 – 2006)

- Professor in Mathematics University of Bergen (1957-1990)
- Cryptographer in WW II
- Pioneer in cryptographer and coding in Norway


E R N S T S. S E L M E R

LINEAR RECURRENCE RELATIONS
OVER FINITE FIELDS

Ernst S. Selmer

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF BERGEN, NORWAY
1966

- Designed error control in Norwegian social security numbers in 1964
- Monograph (1966)
  - "Linear Recurrence Relations over Finite Fields"
  - Sold 200 copies in 10 minutes at Eurocrypt 1993
- Selmer groups & Fermat's theorem
- **First NORCOM, Utstein Kloster, April 1981**

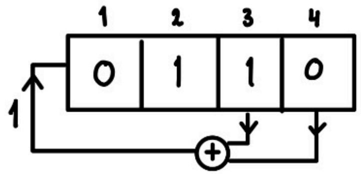
$g(x) \in GF(2^n) \simeq \mathbb{Z}_2[x]/(f(x))$

$g(x) \longmapsto x \cdot g(x) \pmod{f(x)}$

Shift register

(Linear) Feedback Shift Registers LFSR
Golomb – Selmer

i	b_1 (a_i)	b_2	b_3	b_4
-4	1	1	1	1
-3	0	1	1	1
-2	0	0	1	1
-1	0	0	0	1
0	1	0	0	0
1	0	1	0	0
2	0	0	1	0
3	1	0	0	1
4	1	1	0	0
5	0	1	1	0
6	1	0	1	1
7	0	1	0	1
8	1	0	1	0
9	1	1	0	1
10	1	1	1	0
11	1	1	1	1
12	0	1	1	1
13	0	0	1	1
14	0	0	0	1
15	1	0	0	0
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$



$$(a_{-4}, a_{-3}, a_{-2}, a_{-1}) = (1,0,0,0)$$

$$a_n = a_{n-4} + a_{n-3}, \quad i \geq 0$$

$$g = (g_0, g_1, g_2, g_3) \in \mathbb{Z}_2^n$$

$$\downarrow$$

$$(f(g), g_0, g_1, g_2)$$

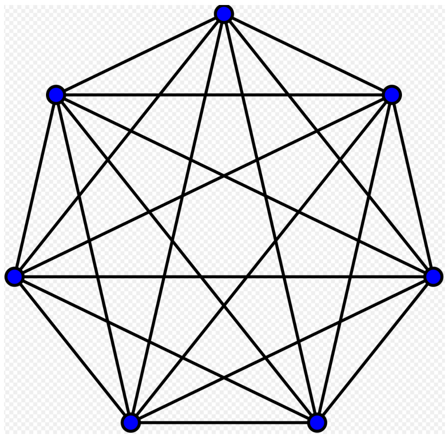
$$f : \mathbb{Z}_2^n \to \mathbb{Z}_2$$

f: feedback function

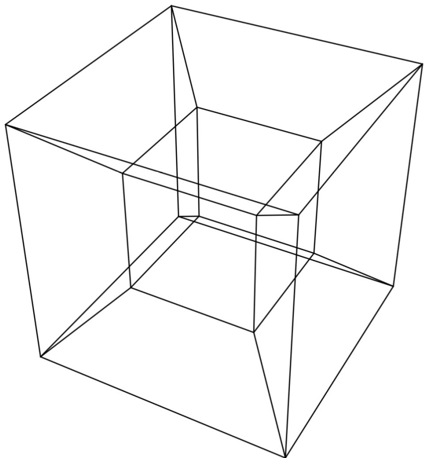
- Linear?
- Non singular?

Permutation networks

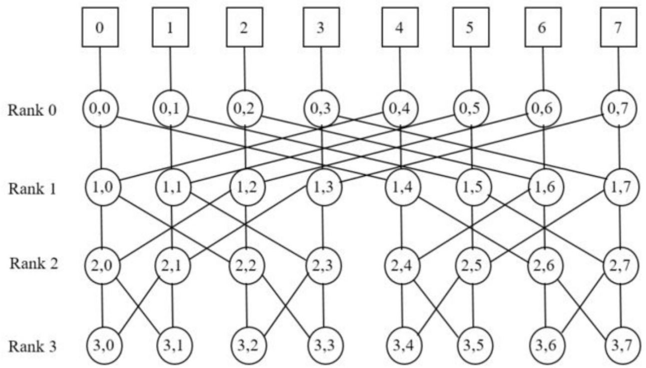
Network	Permuting power	No. of wires	Cost
Complete graph	1	$\Theta(n^2)$	$\Theta(n^2)$
Boolean Cube	$\Theta(\log n)$	$\Theta(n \log n)$	$\Theta(n \log^2 n)$
Butterfly	$\Theta(\log n)$	$\Theta(n \log n)$	$\Theta(n \log^2 n)$
2–D Mesh	$\Theta(\sqrt{n})$	$\Theta(n)$	$\Theta(n\sqrt{n})$
Ring	$\Theta(n)$	$\Theta(n)$	$\Theta(n^2)$
Cube Connected Cycles	$\Theta(\log n)$	$\Theta(n)$	$\Theta(n \log n)$
Shuffle Exchange	$\Theta(\log n)$	$\Theta(n)$	$\Theta(n \log n)$



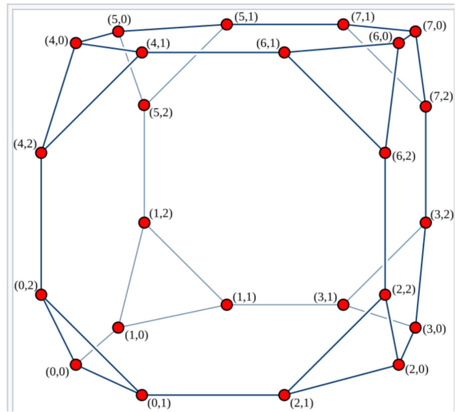
Complete Graph



Boolean Cube (Hypercube)



Butterfly

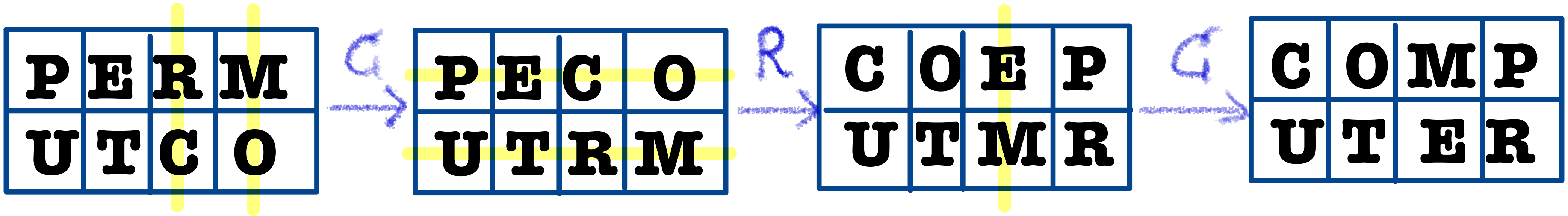


Cube Connected Cycles

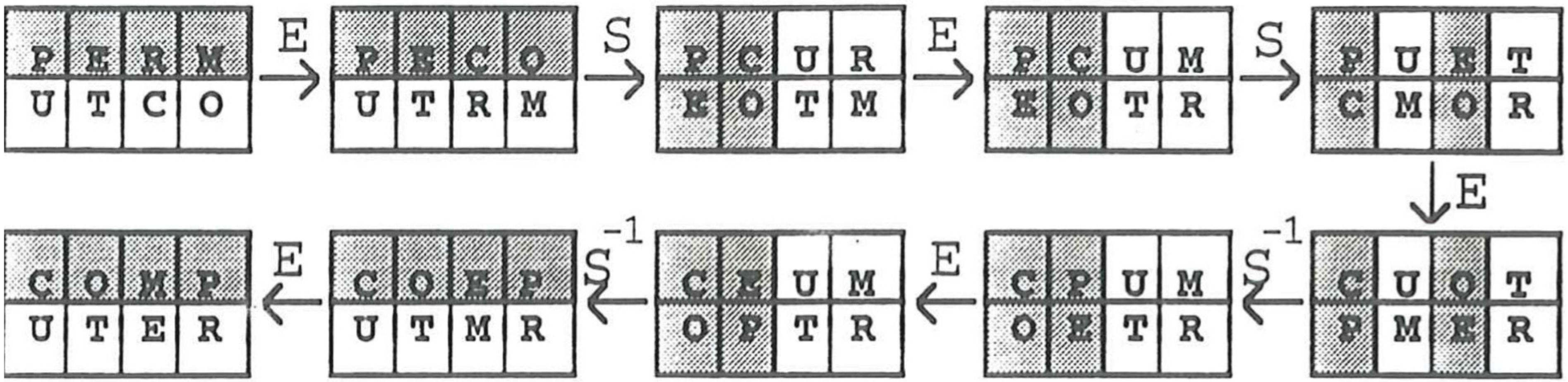
Slepian - Duguid Theorem:

Any permutation of an m x n array can be factorised in
Column_permute o Row_permute o Column_permute

Example: m=2, n=4



Recursive S-D Factorisation, $N=2^n$
Shuffle – Exchange



Coordinates $(g_{n-1},\dots,g_1,g_0)\in\mathbb{Z}_2^n$:

000	100	010	110
001	101	011	111

$$S((g_{n-1},g_{n-2},\dots,g_0)) = (g_{n-2},g_{n-3},\dots,g_0,g_{n-1})$$

$$E((g_{n-1},g_{n-2},\dots,g_0)) = (g_{n-1},g_{n-2},\dots,g_0\oplus 1)$$

$$\Rightarrow \quad \boxed{P = E_{2n-1}S^{-1}E_{2n-2}S^{-1}\cdots S^{-1}E_nSE_{n-1}S\cdots SE_2SE_1}$$

Which mappings S and E can be used?

Theorem. *If $\{S, E\}$ is a pair of permutations satisfying conditions for recursive SD factorisation, then there exists a binary indexing of the elements $g \in \mathcal{G}$:*

$$g = (g_{n-1}, g_{n-2}, \ldots, g_1, g_0), \quad g_i \in \{0, 1\}$$

such that

$$E(g) = (g_{n-1}, g_{n-2}, \ldots, g_1, \overline{g_0}), \qquad \overline{g_0} := g_0 \oplus 1$$
$$S(g) = (g_{n-2}, g_{n-3}, \ldots, g_0, f(g))$$

where f is a boolean function satisfying

$$f(g) = f((g_{n-1}, g_{n-2}, \ldots, g_0)) = h((g_{n-2}, g_{n-3}, \ldots, g_0)) \oplus g_{n-1}.$$

I.e. S is a nonsingular shift register.

Generalised Shuffle Exchange Networks: GSE(n,f)

Q: How design GSE networks? (recursion?)

Theorem. *If f is self-complementary, i.e.*

$$f(g) = f(g^*), \qquad \text{where } g^* = (\overline{g_{n-1}}, \overline{g_{n-2}}, \ldots, \overline{g_0}),$$

then $\phi(g) = g^*$ is the unique non-trivial automorphism of $GSE(n, f)$. Otherwise it has no non-trivial automorphisms.

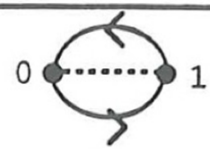
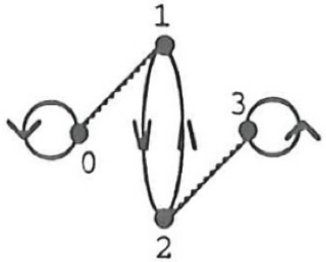
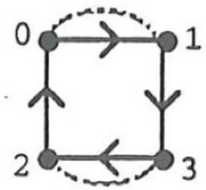
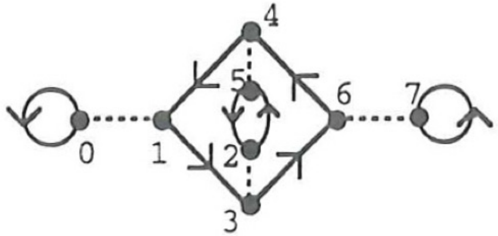
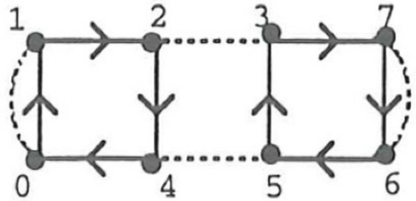
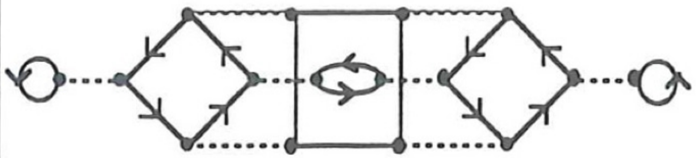
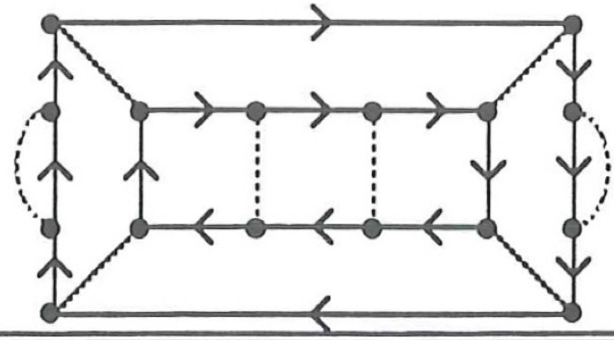
Theorem. *If f is self complementary, then*

$$GSE(n, f)/\phi = GSE(n-1, h)$$

for

$$h(g_{n-2}, g_{n-3}, \ldots, g_0) = f\left(\bigoplus_{i=0}^{n-2} g_i,\ \bigoplus_{i=0}^{n-3} g_i, \ldots,\ g_0,\ 0\right)$$

Maximally foldable GSE-graphs

Character. pol.	Homogenous graph	Inhomogenous graph
$1+x$		
$(1+x)^2 = 1+x^2$		
$(1+x)^3 =$ $1+x+x^2+x^3$		
$(1+x)^4 = 1+x^4$		

Linear recurrencies over finite fields

$$f : \mathbb{Z}_2^n \to \mathbb{Z}_2$$

$$f((g_{n-1}, \ldots, g_0)) = \sum_{i=0}^{n-1} c_i \cdot g_{n-1-i}$$

Linear homogeneous

$$\bar{f}(g) = f(g) \oplus 1$$

Linear inhomogeneous

$$r_f(x) = \sum_{i=0}^{n} c_i \cdot x^i \in \mathbb{Z}_2[x]$$

Characteristic polynomial

$(c_n = 1)$

Lemma:

- f is non-singular $\Leftrightarrow x \nmid r_f(x) \Leftrightarrow r_f(0) = 1$
- f is self-complementary $\Leftrightarrow (x+1) \mid r_f(x) \Leftrightarrow r_f(1) = 0$

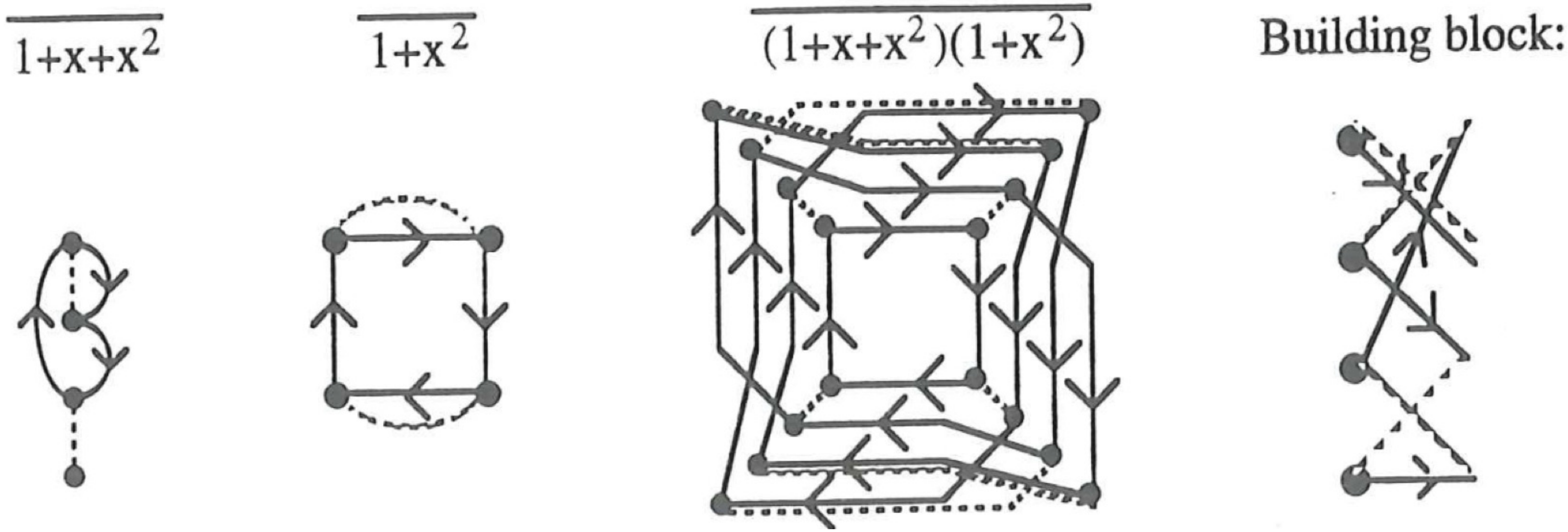
Maximally foldable GSE graphs:

$$GSE(r_f(x)) \text{ and } GSE(\overline{r_f}(x))$$

$$r_f(x) = (1+x)^n$$

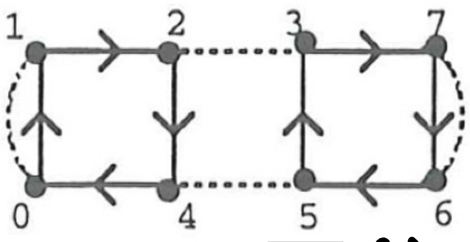
Factorisation of r(x) and graph quotients

If $r(x)=s(x)\cdot t(x)$, $\gcd(s,t)=1$, then $GSE(r) = GSE(s) \times GSE(t)$
direct product



If $r(x)=s(x)\cdot t(x)$, $\gcd(s,t)\neq 1$, then $GSE(r) = GSE(s) \rtimes GSE(t)$

semidirect product



$GSE(\overline{(1+x)}^3)$

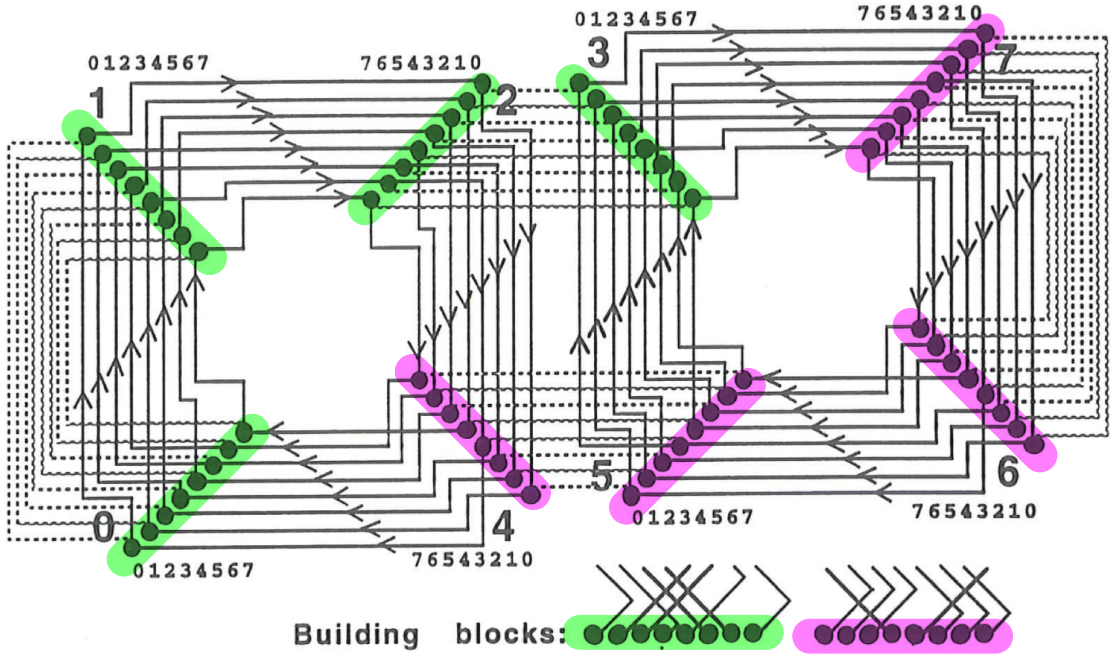


Figure 4: $\mathrm{GSE}(\overline{(1+x)^6})$ as in Theorem 5.7, where $\overline{(1+x)^6} = \overline{(1+x)^3} \cdot \overline{(1+x)^3}$

$$0 \longrightarrow GSE(t) \longrightarrow GSE(r) \xrightarrow{\varphi} GSE(s) \longrightarrow 0$$

Dominique and the Algebra of Shuffles

Dominique has brought a distinctive elegance and warmth to the algebra of shuffles — seeing in them not just combinatorial orderings, but the very rhythm of algebraic structures.

• He explored **shuffle and quasi-shuffle Hopf algebras**, uncovering their role in dendriform and Zinbiel algebras.

• With Sylvie Paycha, he showed how **shuffle relations** govern regularised integrals and multiple zeta values.

• With Kurusch Ebrahimi-Fard and Frédéric Fauvet, he linked **quasi-shuffles** with Écalle's mould calculus — a bridge between words and symmetries.

• In later work, he shaped a **shuffle quadri-algebra**, blending concatenation, deconcatenation, and symmetry into one graceful structure.

For Dominique, shuffles are more than algebra — they are a kind of musical phrasing in mathematics.

Thank you!