Some comments on commutative diagram cryptanalysis

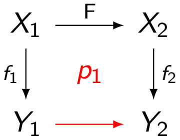
Tim Beyne

KU Leuven and Ruhr University Bochum

April 25, 2024

Commutative diagram cryptanalysis

- Wagner, FSE 2004
- Based on commutative diagrams (cf. categories)



- Every such diagram corresponds to a ‘local property’ of F

Commutative diagram cryptanalysis

- Wagner, FSE 2004
- Based on commutative diagrams (cf. categories)

$$
\begin{array}{ccccc}
X_1 & \xrightarrow{\mathsf{F}} & X_2 & \xrightarrow{\mathsf{F}'} & X_3 \\
{\scriptstyle f_1}\downarrow & \color{red}{p_1} & \downarrow{\scriptstyle f_2} & \color{red}{p_2} & \downarrow{\scriptstyle f_3} \\
Y_1 & \color{red}{\longrightarrow} & Y_2 & \color{red}{\longrightarrow} & Y_3
\end{array}
$$

- Every such diagram corresponds to a ‘local property’ of F
- “Local properties can be pieced together to obtain global properties by exploiting the compositional behavior of commutative diagrams”

Commutative diagram cryptanalysis

- How to define 'probabilistic diagrams'? (i.e. what category)

- *Probabilistic (commutative) diagrams* are not the right notion

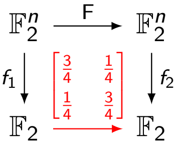
$$
\begin{array}{ccccc}
\mathbb{F}_2^n & \xrightarrow{\mathsf{F}_1} & \mathbb{F}_2^n & \xrightarrow{\mathsf{F}_2} & \mathbb{F}_2^n \\
\downarrow & p_1 = \frac{1}{2} + \frac{c_1}{2} & \downarrow & p_2 = \frac{1}{2} + \frac{c_2}{2} & \downarrow \\
\mathbb{F}_2 & \xrightarrow{\mathsf{id}} & \mathbb{F}_2 & \xrightarrow{\mathsf{id}} & \mathbb{F}_2
\end{array}
$$

- Example: correlation of linear trail is $c_1 c_2$ (not $p_1 p_2$)

- Independence assumption is not good either,
  but the real issue is the definition

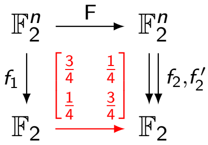
Commutative diagram cryptanalysis

- Wagner's proposal: stochastic commutative diagrams



Commutative diagram cryptanalysis

- Wagner's proposal: stochastic commutative diagrams



- Even if we could define a category where this is a diagram, *stochastic commutative diagram* is an oxymoron

- Many techniques cannot be described in this way, e.g.
  - Integral cryptanalysis
  - No distinction between multiple and multidimensional linear

Probability theory is the wrong framework for cryptanalysis

Motivation for the geometric approach

- Can we at least find a suitable definition for our diagrams?
- ⚠ Even if we have this, we should not expect them to commute
- Mathematically: what category should we work in?
  - Should contain FinSet as a subcategory
  - Must be flexible enough (more flexible than probability theory)
- Strategy of the geometric approach:
  Find a category $\mathcal{C}$ equivalent to FinSet, then enlarge $\mathcal{C}$

Motivation for the geometric approach

Functors $\mathcal{F}$ and $\mathcal{F}^*$

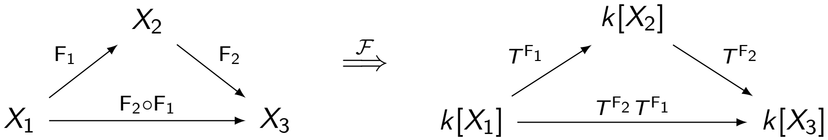
- Vector space $k[X]$ of formal k-linear combinations of X

$$u = \sum_{x \in X} u_x \, x$$

- A function $\mathsf{F} : X \to Y$ has a pushforward $T^{\mathsf{F}} : k[X] \to k[Y]$

$$T^{\mathsf{F}} u = \sum_{x \in X} u_x \, \mathsf{F}(x)$$

- Covariant functor $\mathcal{F}$: FinSet $\to \mathscr{C} \subset k$-FinVect



Motivation for the geometric approach

Functors $\mathcal{F}$ and $\mathcal{F}^*$

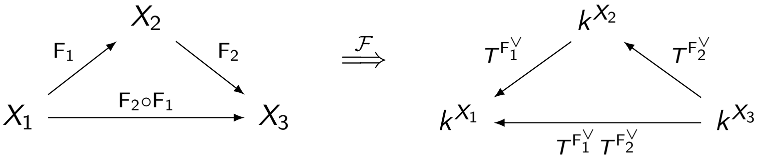
- Vector space k^X of k-valued functions on X

$$v : x \mapsto v(x)$$

- A function $\mathrm{F} : X \to Y$ has a pullback $T^{\mathrm{F}^\vee} : k^Y \to k^X$

$$T^{\mathrm{F}^\vee} v = v \circ \mathrm{F}$$

- Contravariant functor $\mathcal{F}^* : \mathrm{FinSet} \to \mathscr{D} \subset k\text{-FinVect}$



Motivation for the geometric approach

Functors $\mathcal{F}$ and $\mathcal{F}^*$

- Duality between $\mathcal{F} : \mathsf{FinSet} \to \mathscr{C}$ and $\mathcal{F}^* : \mathsf{FinSet}^{\mathsf{op}} \to \mathscr{D}$
- Elements of k^X are also linear functions on $k[X]$:

$$v(u) = \sum_{x \in X} u_x v(x)$$

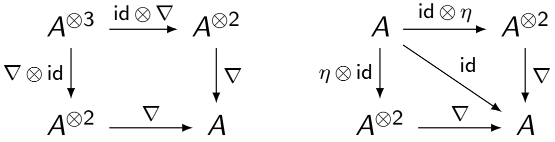
- So we can think of k^X as the dual vector space of $k[X]$
- What are the categories $\mathscr{C}$ and $\mathscr{D} \simeq \mathscr{C}^{\mathsf{op}}$?

Motivation for the geometric approach

Products and coproducts on k^X and $k[X]$

- k^X is an algebra with product $\nabla : k^X \otimes k^X \to k^X$

$$(\nabla(v \otimes w))(x) = v(x)w(x)$$



Motivation for the geometric approach

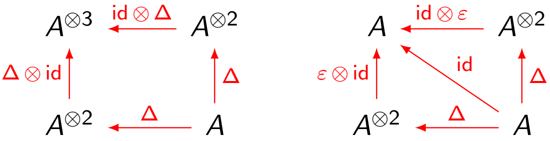
Products and coproducts on k^X and $k[X]$

- k^X is an algebra with product $\nabla : k^X \otimes k^X \to k^X$

$$\big(\nabla(v \otimes w)\big)(x) = v(x)w(x)$$

- $k[X]$ is a coalgebra with coproduct $\Delta : k[X] \to k[X] \otimes k[X]$

$$\Delta(u) = \sum_{x \in X} u_x \, x \otimes x$$



Motivation for the geometric approach

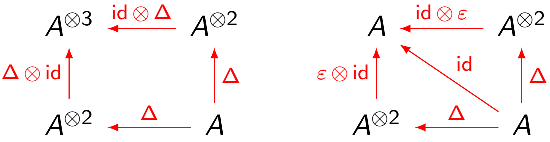
Products and coproducts on k^X and $k[X]$

- k^X is an algebra with product $\nabla : k^X \otimes k^X \to k^X$

$$\big(\nabla(v \otimes w)\big)(x) = v(x)w(x)$$

- $k[X]$ is a coalgebra with coproduct $\Delta : k[X] \to k[X] \otimes k[X]$

$$\Delta(u) = \sum_{x \in X} u_x \, x \otimes x$$



- f is a morphism of algebras if $\nabla \circ (f \otimes f) = f \circ \nabla$
- f is a morphism of coalgebras if $(f \otimes f) \circ \Delta = \Delta \circ f$

Motivation for the geometric approach

Products and coproducts on k^X and $k[X]$

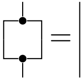
- An algebra is separable if there exists a compatible coproduct
- A coalgebra is coseparable if there exists a compatible product

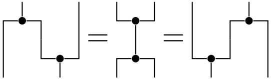
$$\nabla \circ \Delta = \mathrm{id} \qquad (\mathrm{id} \otimes \nabla) \circ (\Delta \otimes \mathrm{id}) = \Delta \circ \nabla = (\nabla \otimes \mathrm{id}) \circ (\mathrm{id} \otimes \Delta)$$

Motivation for the geometric approach
Products and coproducts on k^X and $k[X]$

- An algebra is separable if there exists a compatible coproduct
- A coalgebra is coseparable if there exists a compatible product

$$\nabla \circ \Delta = \mathrm{id} \qquad (\mathrm{id} \otimes \nabla) \circ (\Delta \otimes \mathrm{id}) = \Delta \circ \nabla = (\nabla \otimes \mathrm{id}) \circ (\mathrm{id} \otimes \Delta)$$





- Product and coproduct on k^X and $k[X]$ correspond to copy
  - Product on k^X is $\nabla = T^{\mathrm{copy}^\vee}$
  - Coproduct on $k[X]$ is $\Delta = T^{\mathrm{copy}}$

Motivation for the geometric approach

Functors $\mathcal{F}$ and $\mathcal{F}^*$ as equivalences of categories

- If k is algebraically closed, then

$$\mathsf{FinSet} \overset{\mathcal{F}}{\simeq} \left.\begin{array}{c}\text{finite dimensional}\\ \text{coseparable}\\ \text{cocommutative}\\ k\text{-coalgebras}\end{array}\right\} k\text{-coSepAlg}$$

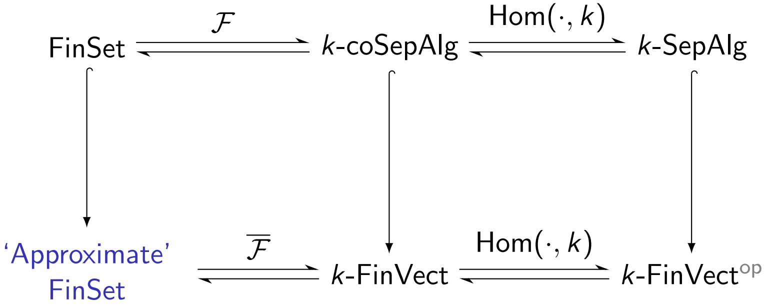
$$\mathsf{FinSet}^{\mathsf{op}} \overset{\mathcal{F}^*}{\simeq} \left.\begin{array}{c}\text{separable}\\ \text{commutative}\\ k\text{-algebras}\end{array}\right\} k\text{-SepAlg}$$

- This has many consequences

Geometric approach

Enlarging the category

- Forgetting the (co)algebra structure leads to more flexibility
- k-FinVect as an indirect but formal setting for cryptanalysis



- 'Probability theory' is somewhere half-way (when $k = \mathbb{R}\dots$)

Geometric approach
Cryptanalytic properties

- Cryptanalytic property for a function $\mathsf{F} : X \to Y$ consists of
  - A subspace $U \subset k[X]$
  - A subspace $V \subset k^Y$
- Cryptanalysis is about evaluating properties:

$$\text{estimating } v(T^{\mathsf{F}} u) \text{ for } u \in U \text{ and } v \in V$$

Geometric approach

Cryptanalytic properties

- Diagrams that commute but don't compose (properties)

$$\begin{array}{ccc} k[X] & \xrightarrow{T^{\mathrm{F}}} & k[Y] \\ \uparrow & \circlearrowright & \downarrow \\ U & \longrightarrow & k[Y]/V^0 \end{array} \quad \text{or dually} \quad \begin{array}{ccc} k^Y & \xrightarrow{T^{\mathrm{F}^\vee}} & k^X \\ \uparrow & \circlearrowright & \downarrow \\ V & \longrightarrow & k^X/U^0 \end{array}$$

Geometric approach

Cryptanalytic properties

- Diagrams that commute but don't compose (properties)

$$\begin{array}{ccc} k[X] & \xrightarrow{T^{\mathrm{F}}} & k[Y] \\ \Big\uparrow & \circlearrowright & \Big\downarrow \\ U & \longrightarrow & k[Y]/V^0 \end{array} \quad \text{or dually} \quad \begin{array}{ccc} k^Y & \xrightarrow{T^{\mathrm{F}^\vee}} & k^X \\ \Big\uparrow & \circlearrowright & \Big\downarrow \\ V & \longrightarrow & k^X/U^0 \end{array}$$

- Diagrams that compose but don't commute (approximations)

$$\sum_i \quad \begin{array}{ccc} k[X] & \xrightarrow{T^{\mathrm{F}}} & k[Y] \\ \Big\uparrow & \not\circlearrowright & \Big\uparrow \\ U & \longrightarrow & V_i^0 \end{array} \quad \text{or dually} \quad \begin{array}{ccc} k^Y & \xrightarrow{T^{\mathrm{F}^\vee}} & k^X \\ \Big\uparrow & \not\circlearrowright & \Big\uparrow \\ V & \longrightarrow & U_i^0 \end{array}$$

- Decomposition $k^Y = \bigoplus_i V_i \Leftrightarrow k[Y] = \bigoplus_i V_i^0$

Geometric approach

Choice of basis

Linear cryptanalysis	Differential cryptanalysis	Integral cryptanalysis
$k = \mathbb{C}$	$k = \mathbb{C}$	$k = \mathbb{C}_p$
X	$X \times X$	X
Commutative group	Commutative group	Commutative inverse monoid

Basis diagonalizes monoid action (for all c in X):

$x \mapsto x + c$	$(x, y) \mapsto (x + c, y + c)$	$x \mapsto cx$

Commutation property of Midori-64

- 'Commutative diagram cryptanalysis made practical'
  Baudrin *et al.*

- $\overline{\gamma}(x) = (\gamma(x_1), \ldots, \gamma(x_{16}))$ commutes with round function

$$\gamma(x) = \begin{cases} x + \mathtt{f} & \text{if } 5^{\mathsf{T}} x = 0 \\ x + \mathtt{a} & \text{else} \end{cases}$$

- As a commutative diagram:

$$\begin{array}{ccc} \mathbb{F}_2^{64} & \xrightarrow{\mathsf{F}} & \mathbb{F}_2^{64} \\ \overline{\gamma} \big\downarrow & \circlearrowright & \big\downarrow \overline{\gamma} \\ \mathbb{F}_2^{64} & \xrightarrow{\mathsf{F}} & \mathbb{F}_2^{64} \end{array}$$

Unusual diagram, due to size of $\mathbb{F}_2^{64}$

Commutation property of Midori-64

Alternative description

- Michiel Verbauwhede independently found this property
- Invariant set of pairs S^{16}

$$S = \left\{ \big(x, \gamma(x)\big) \;\middle|\; x \in \mathbb{F}_2^4 \right\}$$

- Geometric approach: subspace of $k^{\mathbb{F}_2^{64} \times \mathbb{F}_2^{64}}$ spanned by

$$\delta_{S^{16}} = \big(\delta_S\big)^{\otimes 16}$$

- Sparse description in the quasidifferential basis[1]

$$f = \frac{1}{2}\,\delta_0 \boxtimes (\delta_{\mathtt{f}} + \delta_{\mathtt{a}}) + \frac{1}{2}\,\delta_5 \boxtimes (\delta_{\mathtt{f}} - \delta_{\mathtt{a}})$$

[1] $q_{u,a}(x, y) = (-1)^{u^\top x} \delta_a(x + y)$

Commutation property of Midori-64

Probabilistic variant

- Probabilistic property based on the invariant

f	f	f	f
f	f	f	f
f	f	f	f
f	f	f	f

$$\xrightarrow{1}$$

f	f	f	f
f	f	f	f
f	f	f	f
f	f	f	f

Commutation property of Midori-64

Probabilistic variant

- Probabilistic property based on the invariant

f	$\delta_{0,0}$	f	$\delta_{0,0}$
$\delta_{0,0}$	$\delta_{0,0}$	$\delta_{0,0}$	$\delta_{0,0}$
f	$\delta_{0,0}$	f	$\delta_{0,0}$
$\delta_{0,0}$	$\delta_{0,0}$	$\delta_{0,0}$	$\delta_{0,0}$

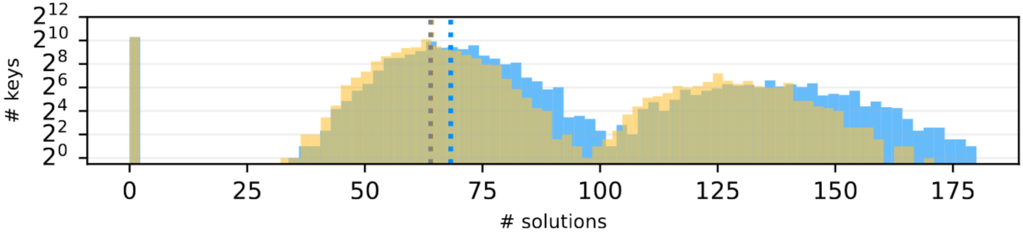
$\xrightarrow{1/16}$

f	$\delta_{0,0}$	f	$\delta_{0,0}$
$\delta_{0,0}$	$\delta_{0,0}$	$\delta_{0,0}$	$\delta_{0,0}$
f	$\delta_{0,0}$	f	$\delta_{0,0}$
$\delta_{0,0}$	$\delta_{0,0}$	$\delta_{0,0}$	$\delta_{0,0}$

- Modify ShiftRows and round constants: $\mathsf{Vert}^2_{\mathsf{SR}}$
- 2^{120} weak keys instead of 2^{96}
- Prediction based on multiplying probabilities: 2^{-4r}

Commutation property of $\mathrm{Vert}^2_{\mathrm{SR}}$

- Estimate of probability 2^{-4r} does not match reality
- For example for $r = 3$ and sample size of 2^{18} pairs:

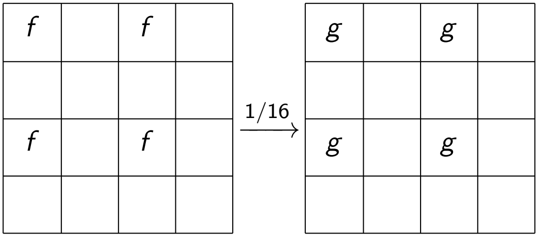


- This is because the analysis ignores important trails

Commutation property of $\mathrm{Vert}^2_{\mathrm{SR}}$

$\mathrm{MC} \circ \mathrm{SR} \circ \mathrm{SC} \circ \mathrm{MC} \circ \mathrm{AK}_k \circ \mathrm{SC} \circ \mathrm{SR} \circ \mathrm{MC}$

- Second approximation for MixColumns with correlation $1/16$



- g is not the indicator function of a set but $g = (\delta_5 \boxtimes \delta_{\mathbb{F}_2^4}) \cdot f$

$$g = \frac{1}{2}\,\delta_0 \boxtimes (\delta_{\mathtt{f}} - \delta_{\mathtt{a}}) + \frac{1}{2}\,\delta_5 \boxtimes (\delta_{\mathtt{f}} + \delta_{\mathtt{a}})$$

- δ_5 is an invariant for two rounds of Midori-64!

Commutation property of $\mathsf{Vert}^2_{\mathsf{SR}}$

MC ∘ SR ∘ SC ∘ MC ∘ AK$_k$ ∘ SC ∘ SR ∘ MC

- g is not an invariant of S, but $D^{\mathsf{S}} g = \big((C^{\mathsf{S}}\delta_5) \boxtimes \delta_{\mathbb{F}_2^4}\big) \cdot f$

$$h_1 = D^{\mathsf{S}} g = \frac{1}{2}(\delta_{14} - \delta_{11}) \boxtimes \delta_{10} + \frac{1}{2}(\delta_{10} + \delta_{15}) \boxtimes \delta_{15}$$

- Still correlation one for the S-box layer

g		g	
g		g	

$\xrightarrow{1}$

h_1		h_1	
h_1		h_1	

Commutation property of $\mathrm{Vert}^2_{\mathrm{SR}}$

$\mathrm{MC} \circ \mathrm{SR} \circ \mathrm{SC} \circ \mathrm{MC} \circ \mathrm{AK}_k \circ \mathrm{SC} \circ \mathrm{SR} \circ \mathrm{MC}$

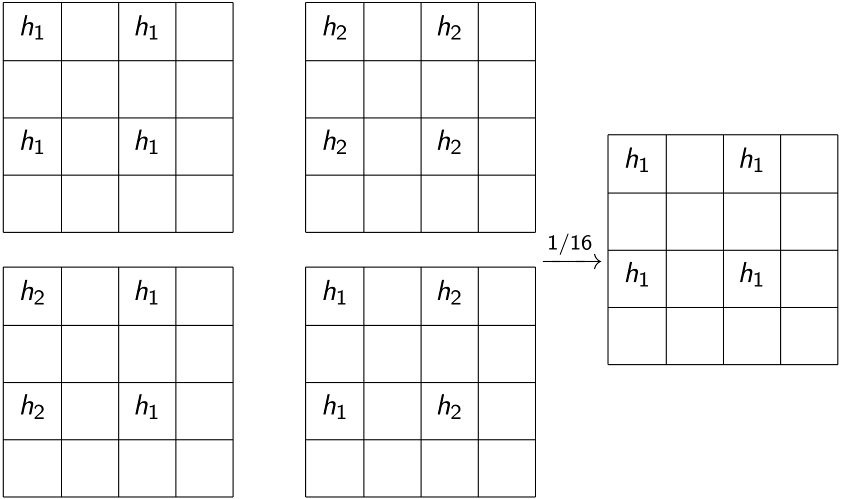
- For k a 4-bit constant such that $\mathtt{5}^\mathsf{T} k = 0$

$$D^k h_1 = (-1)^{\mathtt{b}^\mathsf{T} k} \frac{1}{2} \left((\delta_\mathtt{e} - \delta_\mathtt{b}) \boxtimes \delta_\mathtt{a} - (-1)^{\ \mathtt{1}^\mathsf{T} k} (\delta_\mathtt{a} + \delta_\mathtt{f}) \boxtimes \delta_\mathtt{f} \right)$$

- If $\mathtt{1}^\mathsf{T} k = 1$, then $D^k h_1 = \pm h_1$ (*cf.* invariant)
- If $\mathtt{1}^\mathsf{T} k = 0$, then $D^k h_1 = \pm h_2$

Commutation property of $\text{Vert}^2_{\text{SR}}$

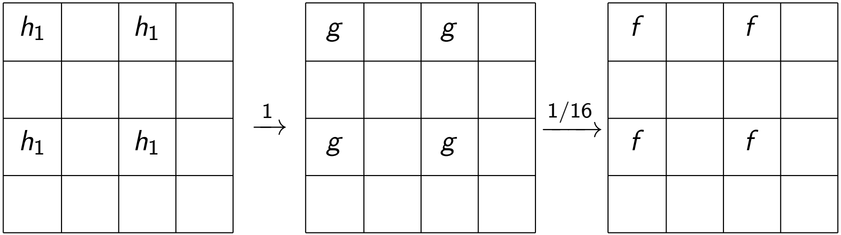
$\text{MC} \circ \text{SR} \circ \text{SC} \circ \text{MC} \circ \text{AK}_k \circ \text{SC} \circ \text{SR} \circ \text{MC}$



- Must have $1^T k_0 = 1^T k_2$ and $1^T k_8 = 1^T k_{10}$

Commutation property of $\mathrm{Vert}^2_{\mathrm{SR}}$

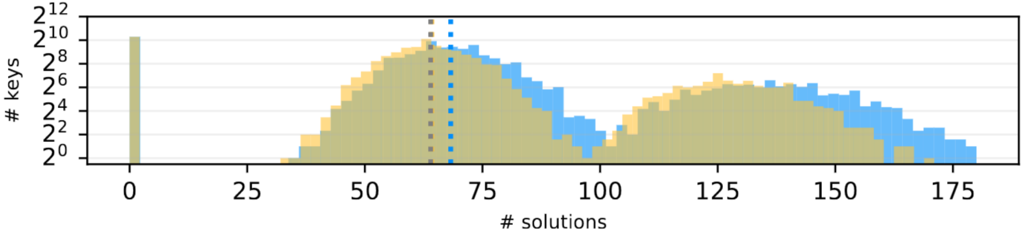
$\mathrm{MC} \circ \mathrm{SR} \circ \mathrm{SC} \circ \mathrm{MC} \circ \mathrm{AK}_k \circ \mathrm{SC} \circ \mathrm{SR} \circ \mathrm{MC}$



Commutation property of $\mathsf{Vert}^2_{\mathsf{SR}}$

- Sum of these trails gives the following probability estimate

$$\frac{1}{2^{12}} \cdot \Big(1 + (-1)^{\mathrm{b}^\top (k_0 + k_2 + k_8 + k_{10})} \delta_0(\mathbf{1}^\top k_0 + \mathbf{1}^\top k_2) \delta_0(\mathbf{1}^\top k_8 + \mathbf{1}^\top k_{10})\Big)$$



- There are some additional trails

- More trails necessary for $r \geq 4$

Conclusions

- Geometric approach ≈ 'forgetting' the (co)algebra structure of finite sets
- Wagner's goal of unification can be achieved but
  - Need to work in a different category (not probabilistic)
  - Diagrams commute but don't compose or
    compose but don't commute
- Acknowledgment
  - J. Baez. Grothendieck–Galois–Brauer Theory
    Blog post (2023)
  - A. Carboni. Matrices, relations, and group representations.
    Journal of Algebra (1991)

`https://tim.cryptanalysis.info/`