Title: Review of recent progress in constructing codes with transversal non-Clifford gates

Speakers: Michael Vasmer

Collection/Series: Quantum Information

Subject: Quantum Information

Date: April 02, 2025 - 11:00 AM

URL: https://pirsa.org/25040104

Abstract:

Quantum codes with transversal non-Clifford gates have many applications in fault tolerant quantum computation, from magic state distillation to robust IQP circuit sampling.
In the past year, there has been spectacular progress on constructing such codes with optimal parameter scaling, i.e., constant encoding rate and constant relative distance.
These constructions rely on quantum versions of algebraic geometry codes, which generalise the well-known Reed-Solomon and Reed-Muller codes.
In this talk, we will describe one such construction that yields a family of good codes with a transversal control-control-Z gate, and we will highlight some of the remaining open problems in this area.

Codes w/ transversal CCZ

Stabilizer code $\mathcal{Q}$ s.t. for encoded states $|\bar{\psi}\rangle, |\bar{\varphi}\rangle, |\bar{\chi}\rangle \in \mathcal{Q}$

$$\overline{CCZ}^{\otimes n} |\bar{\psi}\rangle|\bar{\varphi}\rangle|\bar{\chi}\rangle = \overline{CCZ}^{\otimes k} |\bar{\psi}\rangle|\bar{\varphi}\rangle|\bar{\chi}\rangle$$

Useful for magic state distillation, robust IQP sampling ...

Which codes have this property? What are their parameters?

Pre 2024

$[[n, O(1), \Theta(n^{1/3})]]$ 3D top codes — Bombín, Kubica, Yoshida, Pastawski, MV, Browne

$[[n, \Theta(n), O(1)]]$ Triorthogonal codes — Bravyi, Haah, Campbell, Howard, Krishna, Tillich*

2024 $[[n, \Theta(n), \Theta(n)]]$ Good codes

Wills, Hsieh, Yamasaki 2408.07764

Golowich, Guruswami 2408.09254

Nguyen 2408.10140

Outline

1. Prime power qudits
2. Multiplication property => transversal CCZ
3. AG codes
4. AG codes w/ multiplication property
5. Open questions

Krishna Tillich*

① Prime power qudits

Let F_q finite field w/ $q = 2^m$ elements

Qudits of local dimension q

Basis states $|0\rangle, |1\rangle, \ldots, |q-1\rangle$

$w = e^{2\pi i/2}$

Pauli ops

$\gamma, \beta \in F_q$

$X^\beta |\gamma\rangle = |\gamma+\beta\rangle$

$Z^\beta |\gamma\rangle = w^{tr(\beta\gamma)} |\gamma\rangle$

$tr : F_q \to F_2$

$tr(\alpha) = \alpha + \alpha^2 + \dots + \alpha^{2^{m-1}}$

F_2 linear $\quad tr(\alpha+\beta) = tr(\alpha) + tr(\beta)$

$CCZ|\alpha\rangle|\beta\rangle|\gamma\rangle = (-1)^{tr(\alpha\beta\gamma)}|\alpha\rangle|\beta\rangle|\gamma\rangle$

Can think of those qudits of dimension $q = 2^m$ as m qubits

② Multiplication Property

Def : Star product

Linear code C over F_q

$$C^{*2} = \mathrm{span}_{F_q}\{ x * y : x, y \in C \}$$

$$C^{\perp} = \{ x \in F_q^n : \langle x, y \rangle = 0 \ \forall y \in C \}$$

* component wise multiplication

Def : Multiplication property

$$\boxed{C^{*2} \subseteq C^{\perp}}$$

Krishna Tillich*

$\forall\, x, y, z \in C$

$|x * y * z\rangle := \sum_{i=1}^{n} x_i y_i z_i = 0$

Lemma: C has mult. property $[n, k, d]$

$(1, 1, \ldots, 1) \in C$

We can construct a CSS code Q $[[N, K, D]]$

w/ transversal CCZ.

Proof

Let G be the generator matrix of C

$$G = \begin{pmatrix} — & x_1 & — \\ — & x_2 & — \\ & \vdots & \\ — & x_k & — \end{pmatrix}$$

↓ Gaussian elimination

$K \leq k$

$$\begin{pmatrix} 1_K & G_1 \\ 0 & G_0 \end{pmatrix}$$

$$G' := \begin{pmatrix} G_1 \\ G_0 \end{pmatrix}$$

$$|G'_a * G'_b * G'_c| = \begin{cases} 1 & a=b=c \in \{1,\dots,K\} \\ 0 & \text{otherwise} \end{cases}$$

Notation

$G' = \text{rowspan}(G')$

$G_0 = \text{rowspan}(G_0)$

G_1 " " " G_1

$|\bar{\alpha}\rangle \propto \sum_{g \in G_0} |\alpha G_1 + g\rangle$

$\alpha \in \mathbb{F}_q^k$

$|\underline{x}\rangle \propto \sum_{S \in S_X} \bar{X}_1^{x_1} \cdots \bar{X}_k^{x_k} S|0\rangle^{\otimes n}$

Can show Q has params

$[[N = n-K, K, D]]$ $\quad D = \min_{g \in G_0^\perp \setminus G'} |g|$

Define CSS code Q

X stabilizers G_0

Z stabilizers $G'^\perp$

Krishna Tillich*

$$CCZ^{\otimes N}\,|\bar{\alpha}\rangle|\bar{\beta}\rangle|\bar{\gamma}\rangle$$

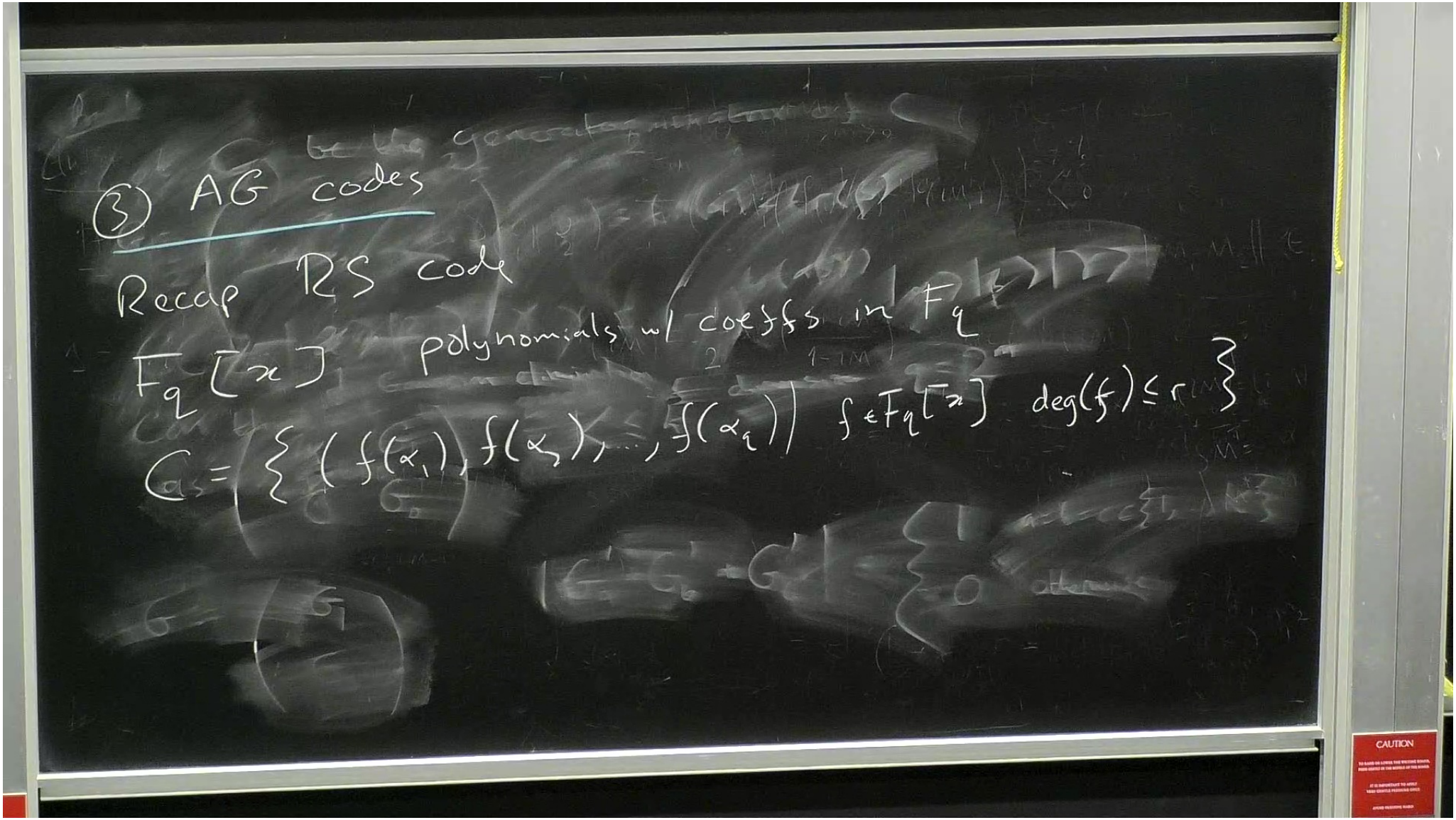
$$\propto \sum_{g,g',g''} (-1)^{\sum_{i=1}^{N} \mathrm{tr}[(\alpha G_1+g)_i\,(\beta G_1+g')_i\,(\gamma G_1+g'')_i]}\,|\alpha G_1+g\rangle|\beta G_1+g'\rangle|\gamma G_1+g''\rangle$$

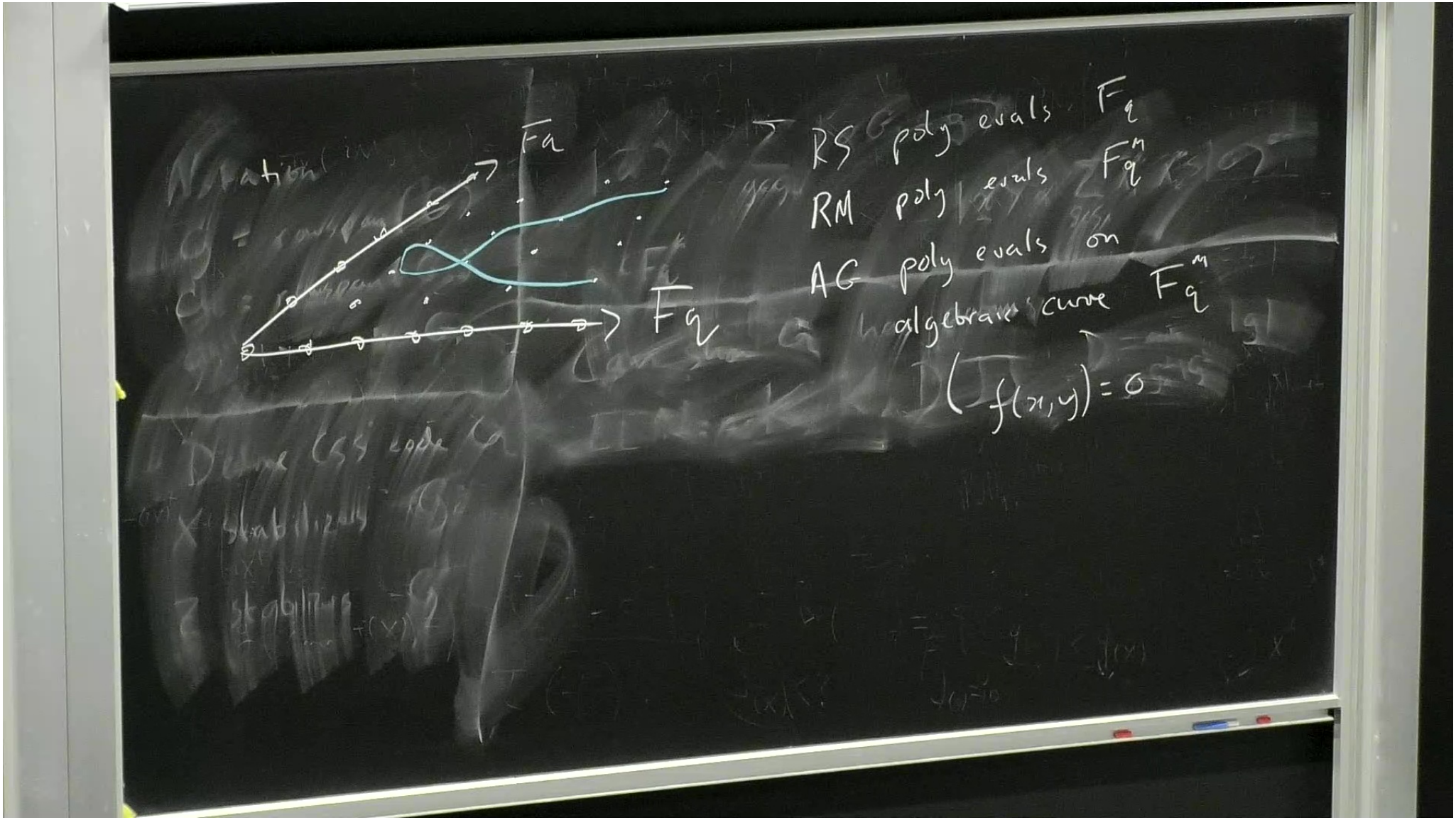
$CCZ \times 11\; CCZ \times 11$
$X \circ CZ \times 11$
$1 \circ CZ$

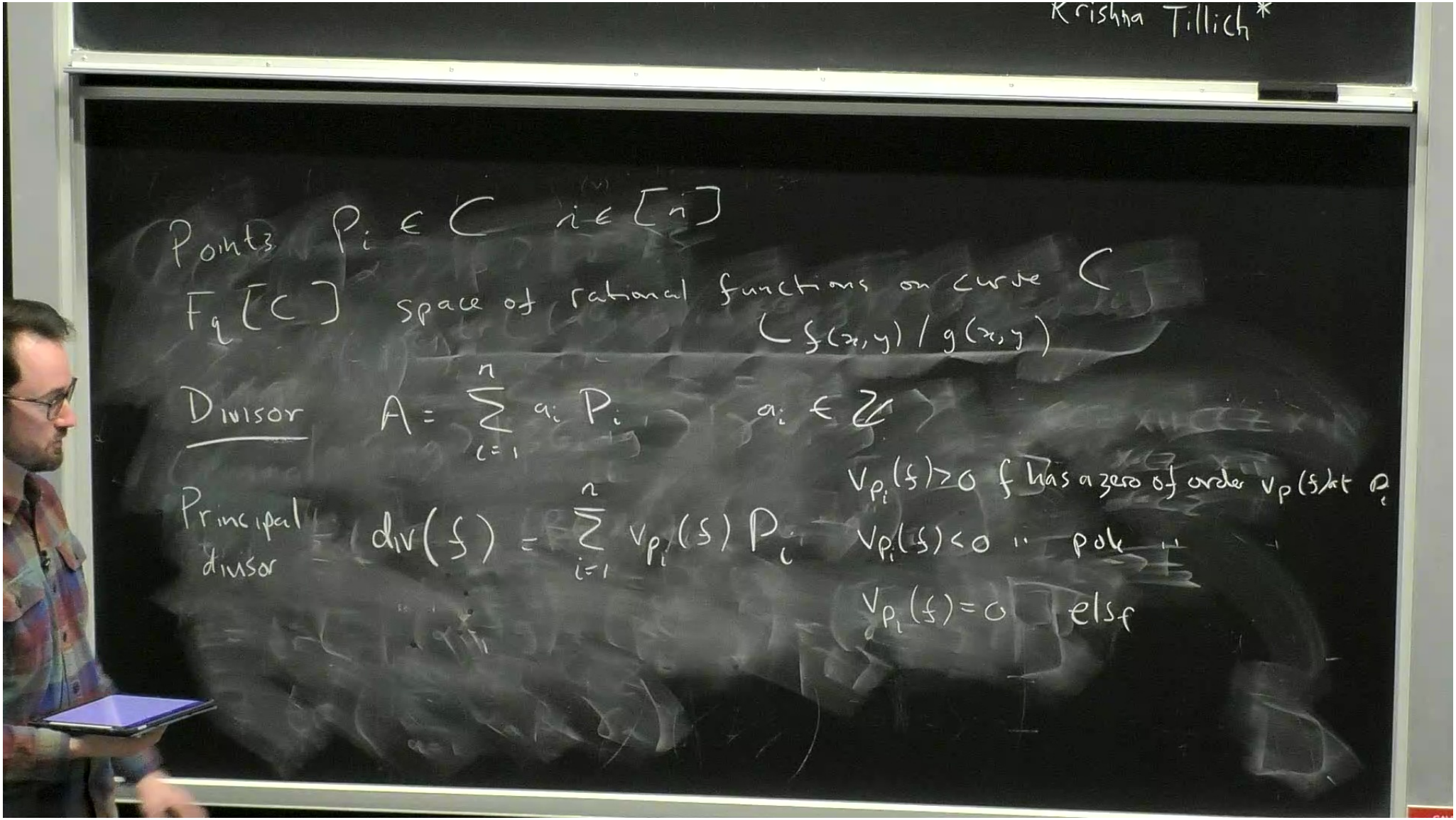
$$\mathrm{tr}\Big[\sum_{i=1}^{N} (\alpha G_1+g)_i\,(\beta G_1+g')_i\,(\gamma G_1+g'')_i\Big]$$

$$= \mathrm{tr}\Big[\,|\,(\alpha G_1+g)*(\beta G_1+g')*(\gamma G_1+g'')\,|\,\Big]$$

$$\doteq \mathrm{tr}\Big(\sum_{a=1}^{K} \alpha_a \beta_a \gamma_a\Big)$$


(3) AG codes
Recap RS code
$\mathbb{F}_q[x]$ polynomials w/ coeffs in $\mathbb{F}_q$
$C_S = \{ (f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)) \mid f \in \mathbb{F}_q[x] \ \deg(f) \leq r \}$


F_q
F_q
RS poly evals F_q
RM poly evals F_q^m
AG poly evals on
algebraic curve F_q^m
$f(x,y) = 0$


Krishna Tillich*
Points $P_i \in C$ $i \in [n]$
$F_q[C]$ space of rational functions on curve C
$\frac{f(x,y)}{g(x,y)}$
Divisor $A = \sum_{i=1}^{n} a_i P_i$ $a_i \in \mathbb{Z}$
Principal divisor $div(f) = \sum_{i=1}^{n} v_{P_i}(f) P_i$
$v_{P_i}(f) > 0$ f has a zero of order $v_P(f)$ at P_i
$v_{P_i}(f) < 0$ " pole "
$v_{P_i}(f) = 0$ else

(3) AG codes

Riemann–Roch space

$$\mathcal{L}(A) = \{ f \in F_q[C] : \mathrm{div}(f) + A \geq 0 \}$$

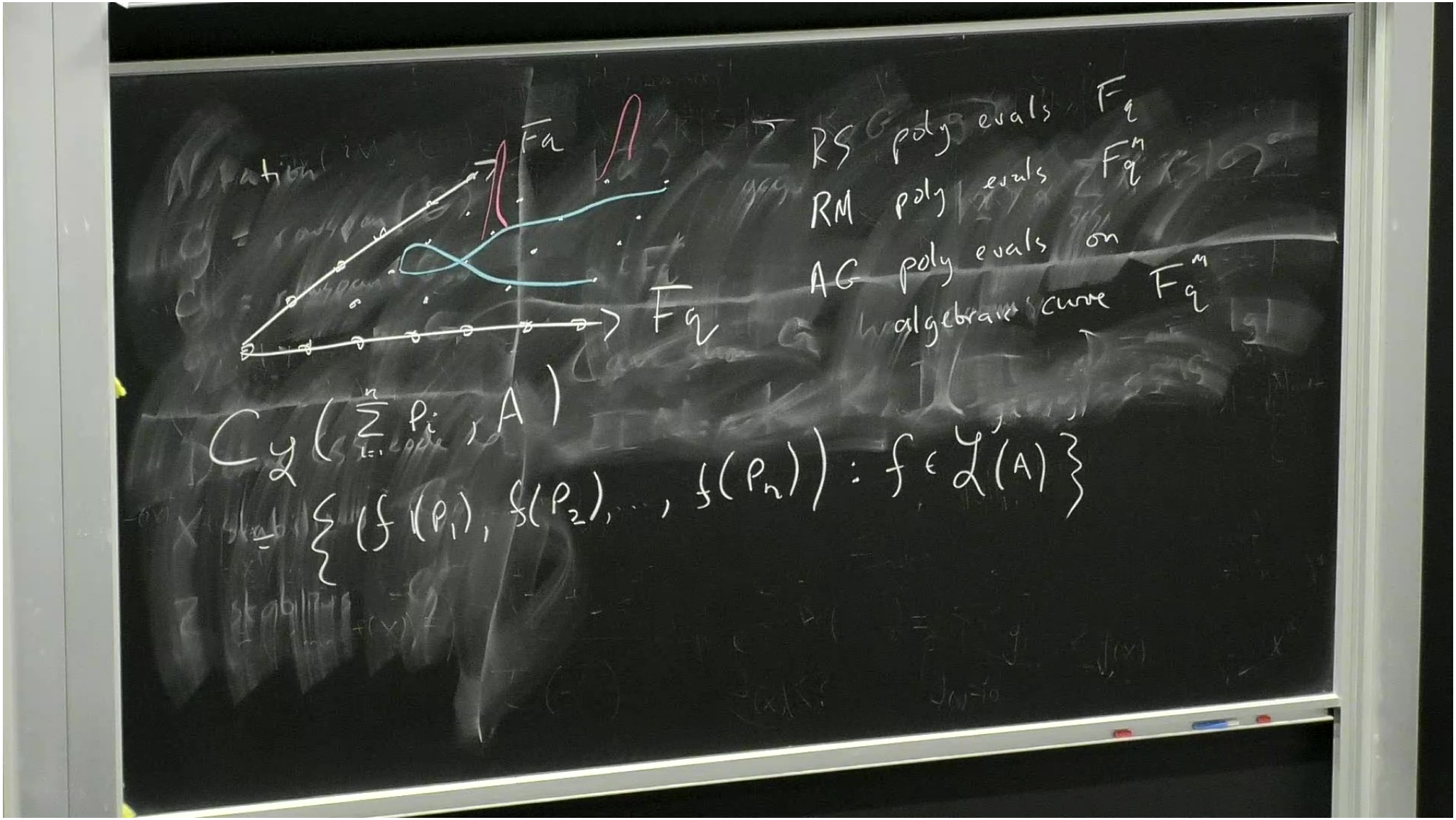
$$\left(A = \sum_i a_i P_i \right)$$

$$v_{P_i}(f) + a_i \geq 0$$

f can only have poles at points P_i where $a_i > 0$

$\deg(f) \leq$

otherwise


F_q
A
F_q
RS poly evals F_q
RM poly evals F_q^m
AG poly evals on algebraic curve F_q^m
$C_{\mathcal{L}}\left(\sum_{i=1}^{n} P_i, A\right)$
$\left\{\left(f(P_1), f(P_2), \ldots, f(P_n)\right) : f \in \mathcal{L}(A)\right\}$

Krishna Tillich*

Ex RS codes

C projective line over F_q

$P_1 = \alpha_1, \ldots, P_q = \alpha_q \quad P_\infty$

$A = r P_\infty$

$\mathcal{L}(A)$ contains functions with poles of order at most r at P_∞

$f(x) = x^2$