Some examples of how finite fields can be useful

Samuel Abreu
CERN & The University of Edinburgh

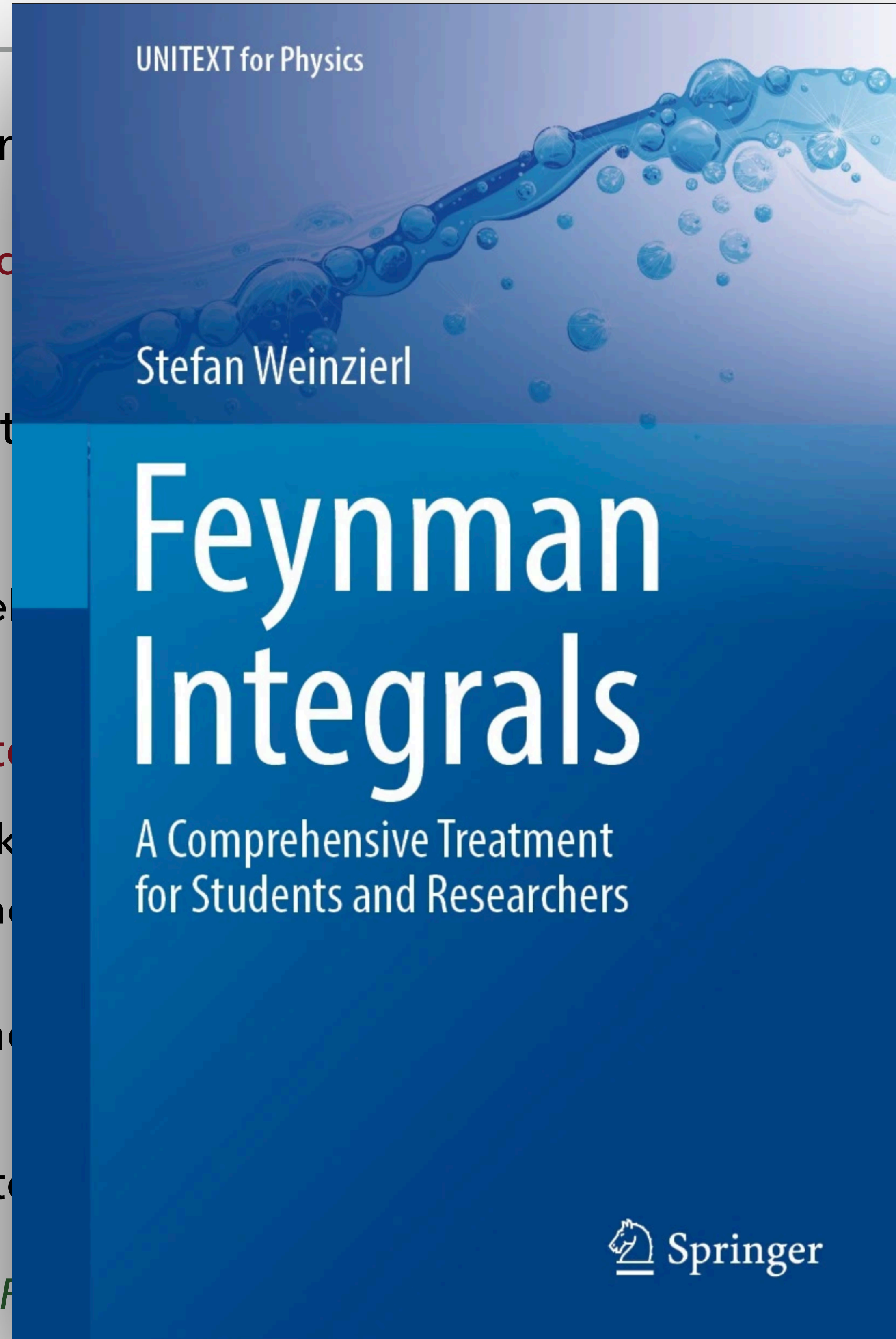
NISER Bhubaneswar — ASWMSA 2024

Introduction

- Advanced tools to compute Feynman integrals/amplitudes. Why is it still hard?
  - Master equation: decomposition in terms of master integrals $$G = \sum_i c_i m_i$$
- How do we compute the c_i? Linear relations between Feynman integrals
  - IBP relations
  - Dimension-shift relations
- Solve large linear systems
  - Often a bottleneck!
  - We will discuss one approach to solve this, applicable beyond this context
- Not discussed here: how to compute the m_i
- Everything you want to know about Feynman integrals: many reviews, such as
  - *Analytic Tools For Feynman Integrals*, V.A. Smirnov (Springer, 2012)
  - *Feynman Integrals (A **Comprehensive** Treatment for Students and Researchers)*, S.Weinzierl (Springer, 2022)

Introduction

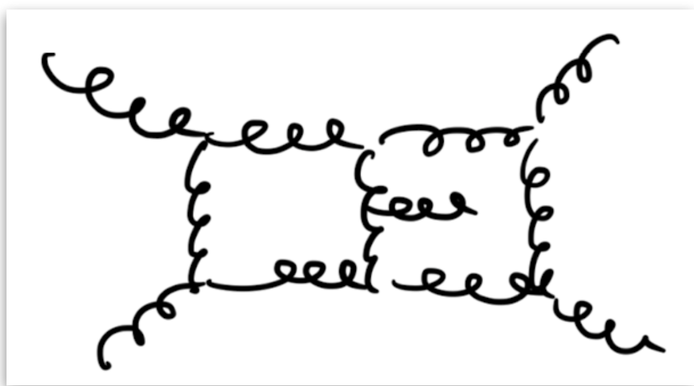
- Advanced tools to cor… …Why is it still hard?
  - Master equation: c… $G = \sum_i c_i m_i$



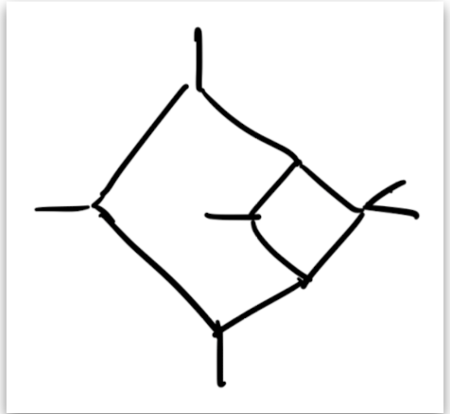
- How do we compute t… …n integrals
  - IBP relations
  - Dimension-shift re…
- Solve large linear syst…
  - Often a bottleneck…
  - We will discuss one… …his context
- Not discussed here: h…
- Everything you want t… …reviews, such as
  - *Analytic Tools For F…* …12)
  - *Feynman Integrals (A **Comprehensive** Treatment for Students and Researchers)*, S.Weinzierl (Springer, 2022)

Motivation

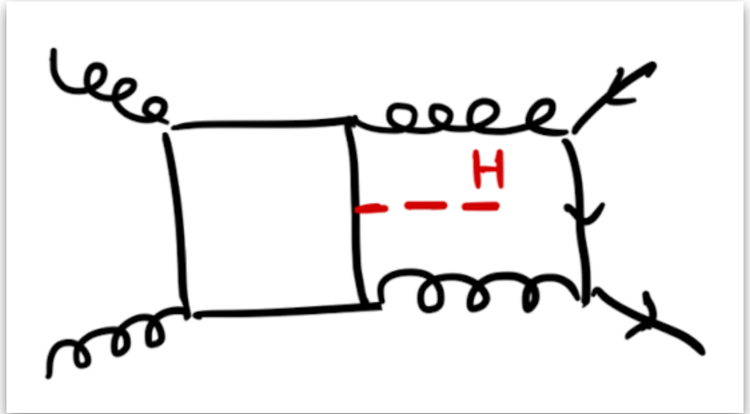
✓ Multi-loop amplitudes and integrals that depend on many scales



3-jet production at LHC



2-loop 5-pt one mass integrals



Higgs + 2-jet production at LHC

- If not careful, expressions get too large to handle in analytic form
- Requires special tools compared to quantities depending on fewer scales
- Use of finite-field based techniques has been crucial for the great progress in these calculations

[many tools implement these techniques: FiniteFlow, Caravel, FireFly, ...]

What is a finite field?

- A field $\mathbb{F}_p$ with a finite set of p elements, equipped with two (four) operations. If $a, b \in \mathbb{F}_p$
  - addition $a + b \in \mathbb{F}_p$
  - multiplication $a \,.\, b \in \mathbb{F}_p$
  - subtraction $a - b \in \mathbb{F}_p$
  - division $a/b \in \mathbb{F}_p$
- There is an additive and multiplicative inverse, $-a$ and a^{-1}
  - $a + (-a) = 0$
  - $a \,.\, a^{-1} = 1$
- Concrete representation: the (positive) integers modulo a prime number, equipped with the standard addition and multiplication
- Example: $\mathbb{F}_5$, the set $\{0,1,2,3,4\}$
  - $2^{-1} = -2 = 3 \mod 5\,;$
  - $-4 = 1\,;\, 4^{-1} = 4 \mod 5\,;$

Why use finite fields?

- Rational numbers have a unique image in a finite field
  - E.g. $\frac{1}{37} = 3\,, \quad \frac{3}{152} = \frac{37}{13} = 4 \quad \mod 5$
  - Can be used to numerically evaluate rational expressions **exactly**
  - The inverse operation is not unique, more on this later

- Any rational number is represented by an integer of fixed maximum size
  - By choosing p, we can control the size of the integers we need to handle

- Can implement very efficient and exact linear algebra algorithms over a finite field (using the fact that all numbers fit exactly on a computer)
  - $\mathbb{F}_p$ with $p = 2^{31} - 1$ for 32-bit numbers
  - $\mathbb{F}_p$ with $p = 2^{63} - 25$ for 64-bit numbers

- If we ask the right question, and the finite field is large enough, answer is the same as for rational numbers
  - e.g.: compute the rank of matrices
  - Verify correctness by evaluating in a second finite field

When to use/not use finite fields? (some examples)

- ✓ 😀 When only rational functions are involved
  - Can be exactly represented in the finite field
  - Not always what we see in practice, but there are ways around it
- ✓ 😀 When the results are *simple*
  - Result in the finite field is likely to be easily lifted to rational numbers
- ✓ 🙁 Numerical evaluations for e.g. Monte Carlo integration
  - Other functions are involved that cannot be represented in a finite field
  - Complicated numerical points require a lot of finite-field evaluations
- ✓ 🙁 To compute limits of expressions
  - There is no natural concept of distance in a finite field

It usually takes some effort to formulate a problem in a way where it can be approached with finite fields

Functional reconstruction

$$G = \sum_i c_i m_i \qquad\qquad c_i = \frac{P(x_1, \ldots, x_n)}{Q(x_1, \ldots, x_n)}$$

[e.g., Peraro, JHEP **1612** (2016) 030]

- Goal: determine the c_i from numerical evaluations
  - Assume P and Q are polynomial in the x_k over the rational numbers
- Step 1: write the most general ansatz for the polynomials

$$P(x_1, \ldots, x_n) = d + d_1 x_1 + \ldots + d_{11} x_1^2 + d_{12} x_1 x_2 + \ldots$$

- Step 2: generate numerical data in $\mathbb{F}_p$, and solve large linear system to constrain ansatz
  - Solves the problem in $\mathbb{F}_p$
  - Note: Scales badly with the number of variables and degree of polynomials, very important to be smart when writing the ansatz
- Step 3: lift the solution from $\mathbb{F}_p$ to the field of rational numbers
  - Rational reconstruction

Rational reconstruction and Chinese remainder theorem

$$P(x_1, \ldots, x_n) = d + d_1 x_1 + \ldots + d_{11} x_1^2 + d_{12} x_1 x_2 + \ldots$$

[e.g., Peraro, JHEP **1612** (2016) 030]

- ✓ Goal: determine the $d_{\ldots}$ from their image in $\mathbb{F}_p$
  - Answer is not unique!

$$\frac{3}{152} = \frac{37}{13} = 4 \mod 5$$

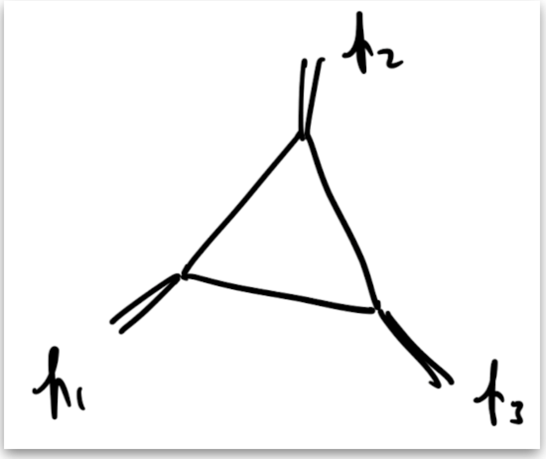
- ✓ Use extended Euclidean algorithm to determine $d_{\ldots}$
  - Guess likely correct if $d_{\ldots} = \frac{a}{b}, \quad a^2, b^2 \lesssim p$
- ✓ If there are worries, check in second finite field $\mathbb{F}_n$
- ✓ If rational reconstruction failed: use Chinese remainder theorem
  - Combine evaluations in $\mathbb{F}_p$ and $\mathbb{F}_n$ to get evaluation in $\mathbb{F}_{pn}$
  - Maintains advantage of `small' finite fields
  - Systematically brings us closer to satisfy the criterium for rational reconstruction
- ✓ If number we are targeting is hard, will need a lot of finite-field evaluations!
  - Target quantities that are expected to be simple!

What about square roots?

- Don't appear in IBPs, but appear in pure basis of master integrals and their DEs
  - Example: three-mass one-loop triangle leading singularity is $\sqrt{\lambda(p_1^2, p_2^2, p_3^2)}$

$$\partial_{p_i^2}\sqrt{\lambda(p_1^2, p_2^2, p_3^2)}\, T(p_1^2, p_2^2, p_3^2) = \frac{T(p_1^2, p_2^2, p_3^2)}{2\sqrt{\lambda(p_1^2, p_2^2, p_3^2)}}\partial_{p_i^2}\,\lambda(p_1^2, p_2^2, p_3^2) + \ldots$$

  - Coefficients in the DE do have square roots in them…



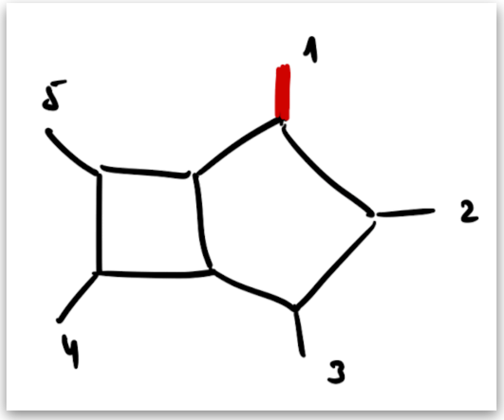
- Can I compute a square-root in a finite-field?
  - No, because it's not part of the operations we have …

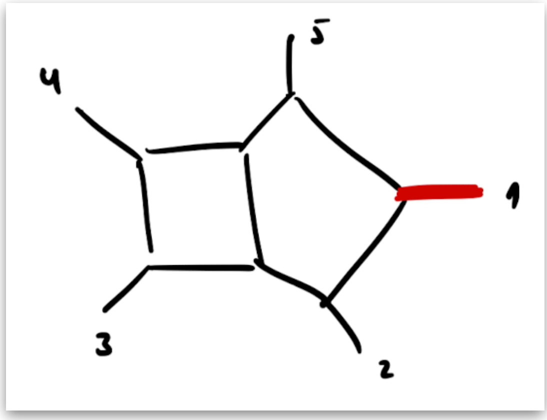
- However, can check if the equation $a^2 = b$ has solutions in $\mathbb{F}_p$
  - If a solution exists, b is a quadratic residue $\mod p$
  - If b is a quadratic residue, can compute the `square root'
  - Use e.g. Tonelli-Shanks algorithm to find a
  - Example: $(1823712)^2 = 1620773388 \mod 2^{31} - 1$

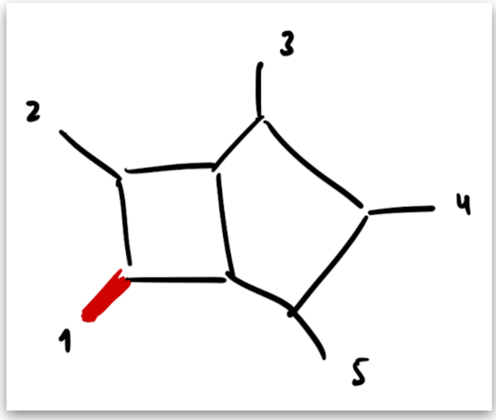
- How many quadric residues exist? For $p > 2$, there are $(p+1)/2$ (~ half the elements)
  - Easy to find: pick points randomly and have 50% chance to land on quadratic residue!

Example 1

- Planar five-point one-mass scattering at two-loops





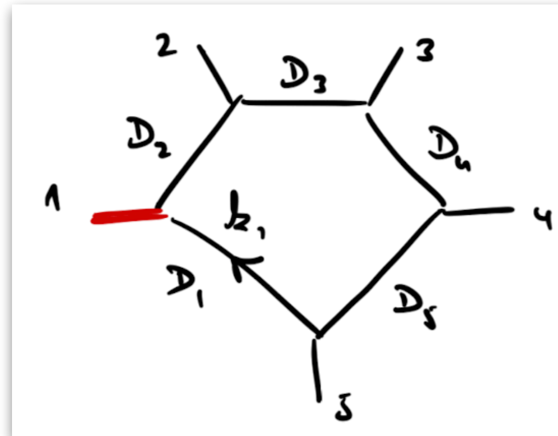


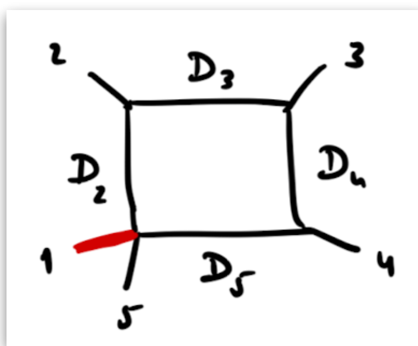
- This set of integrals has a fixed ordering of the massless legs
- For an amplitude, need *all permutations* of the massless legs $\{p_2, p_3, p_4, p_5\}$
- Singularities of these integrals tell us a lot about them: $d\log$ forms (aka, alphabet)

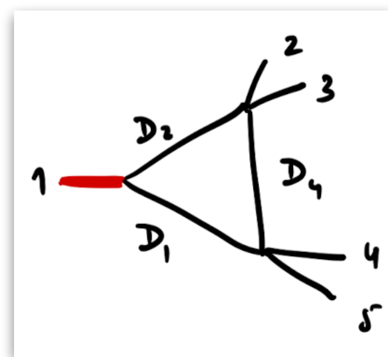
- If I know the singularities of the representative integrals above, how do I generate an independent set of $d\log$ forms describing the singularities of the integrals in all permutations?

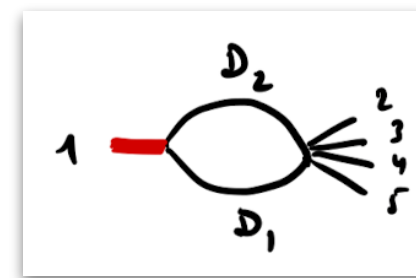
Example 2

- Differential equations for the pentagon with a single massive external leg









- Good basis

$$\Big\{\epsilon^3\sqrt{\Delta_5}\,F^{6-2\epsilon}[1,1,1,1,1],$$

$$\epsilon^2 s_{23}s_{34}\,F[0,1,1,1,1],\epsilon^2 s_{34}s_{45}\,F[1,0,1,1,1],\epsilon^2 s_{15}s_{45}\,F[1,1,0,1,1],\epsilon^2(s_{12}s_{15}-p_1^2 s_{34})\,F[1,1,1,0,1],\epsilon^2 s_{12}s_{23}F[1,1,1,1,0]\,,$$

$$\epsilon^2\sqrt{\lambda(p_1^2,s_{23},s_{45})}\,F[\{1,1,0,1,0\}],$$

$$(1-2\epsilon)\epsilon\,F[1,1,0,0,0],(1-2\epsilon)\epsilon\,F[1,0,1,0,0],(1-2\epsilon)\epsilon\,F[0,1,0,1,0],(1-2\epsilon)\epsilon\,F[0,0,1,0,1],$$

$$(1-2\epsilon)\epsilon\,F[1,0,0,1,0],(1-2\epsilon)\epsilon\,F[0,1,0,0,1]\,\Big\}$$

Example 2

[Abreu, Ita, Moriello, Page, Tschernow, Zeng, 20]

$$d\vec{\mathcal{J}}(x,\epsilon) = \epsilon\, M(x)\, \vec{\mathcal{J}}(x,\epsilon)$$

$$M(x) = \sum_i M_\alpha\, d\log W_\alpha$$

- ✓ DE in a random direction:

$$\vec{c}\cdot\frac{\partial}{\partial\vec{s}}\vec{\mathcal{J}} = \mathbf{C}(\epsilon,\vec{s}\,)\,\vec{\mathcal{J}} \qquad \mathbf{C}(\epsilon,\vec{s}\,) = \epsilon\sum_\alpha M_\alpha\,\vec{c}\cdot\frac{\partial}{\partial\vec{s}}\log(W_\alpha)\,.$$

- ✓ For numerical kinematics and a random $\vec{c}$, $\mathbf{C}(\epsilon,\vec{s}\,)$ is a matrix of numbers
  - Flatten $\mathbf{C}(\epsilon,\vec{s}^{\,k})$ into a vector, collect several such vectors into a matrix
  - Rank of this matrix is the number of independent letters!

- ✓ Assume over complete set of letters is known: how to determine the M_α?
  - Find which letters contribute: row reduction (like in Example 1)
  - Evaluate $\mathscr{W}_{\alpha k} = \vec{c}\cdot\left[\frac{\partial}{\partial\vec{s}}\log(W_\alpha)\right]\Big|_{\vec{s}=\vec{s}^{(k)}}$
  - The matrices of rational numbers are $M_\alpha = \sum_k \mathscr{W}^{-1}_{\alpha,k}\mathbf{C}(\vec{s}^{(k)})$

CONCLUDING REMARKS

Concluding Remarks

- ✓ Finite Fields are a tool
  - Particularly useful to explore properties of linear systems
- ✓ Very useful in function/rational reconstruction problems
- ✓ They don't do magic: as with all tools, they are helpful for certain classes of problems
  - Sometimes it takes some effort to formulate a problem in the right way
- ✓ Useful beyond Feynman integral/amplitude calculation
  - Useful technique to handle big expressions, wherever they appear

THANK YOU!