北京大学
PEKING UNIVERSITY

基于有限域的数值重构方法

何传奇

Advisor：Y-Q.Ma

Outline

01 • 有理数重构

02 • 函数重构

03 • 应用

Introduction

- the high accuracy expected from experimental data which is being collected at the Large Hadron Collider(LHC)

- calculation of loop amplitudes —— rewrite them as a linear combination of loop integrals.

- While the coeffcients of this linear combination are rational functions of kinematic invariants, the loop integrals can instead be computed in terms of special functions.

有理数重构算法

域

假设 <A,+,*> 是一个代数系统，其中，+和 * 都是集合 A 上的二元运算，如果满足：

（1）<A,+> 是交换群（Abel群）；

（2）<A-{e}, + >也是交换群（Abel群）；

（3） * 对+ 是可分配的；

则称 <A,+,*> 是一个域。

整数（环）

有理数，实数，复数，有理函数

$\mathbb{Z}_n = \{0, \ldots, n-1\}.$ Z_{67}

有限域 （加法n阶循环群）

有理数重构算法

```
In[1]:= ModularInverse[43, 67]
        模逆
Out[1]= 53

In[2]:= Mod[43 * %, 67]
        模余
Out[2]= 1
```

$$q = a/b \in \mathbb{Q},$$

$$q \bmod p \equiv \left(a \times \left(b^{-1} \bmod p\right)\right) \bmod p.$$

```
In[3]:= RatMod[nume_, deno_, p_] := Mod[ModularInverse[deno, p] Mod[nume, p], p];
                                    模余 模逆                    模余

        RatMod[2, 5, 67] (* 2/5 在有限域Z67的像是54*)

Out[5]= 54
```

原像的不唯一性

- 问：我要怎么找有限域数的有理数原像？
- 给定有限域的一个数，它的有理数原像有无穷多个，而且在实数平面上稠密

```
In[17]:= p = Prime[10000]
          素数
Out[17]= 104729

In[18]:= Sqrt[p / 2.]
          平方根
Out[18]= 228.833
```

$$a^2, b^2 \lesssim n.$$

所有分子分母绝对值不大于228的有理数个数

```
In[19]:= Table[i / j, {i, -228, 228}, {j, 1, 228}] // Flatten // Union // Length
          表格                                      压平      并集      长度
Out[19]= 63351
```

投影到有限域的整数个数

```
In[20]:= Table[RatMod[i, j, p], {i, -228, 228}, {j, 1, 228}] // Flatten // Union // Length
          表格                                                 压平      并集      长度
Out[20]= 63351
```

像与原像的一一对应

```
In[7]:= Sqrt[67. / 2]
        |平方根
Out[7]= 5.78792
```

Z_{67}

```
In[8]:= Table[i / j, {i, -5, 5}, {j, 1, 5}]
        |表格
        Table[RatMod[i, j, 67], {i, -5, 5}, {j, 1, 5}]
        |表格
```

$$\left\{\left\{-5,-\frac{5}{2},-\frac{5}{3},-\frac{5}{4},-1\right\},\left\{-4,-2,-\frac{4}{3},-1,-\frac{4}{5}\right\},\left\{-3,-\frac{3}{2},-1,-\frac{3}{4},-\frac{3}{5}\right\},\left\{-2,-1,-\frac{2}{3},-\frac{1}{2},-\frac{2}{5}\right\},\right.$$
$$\left.\left\{-1,-\frac{1}{2},-\frac{1}{3},-\frac{1}{4},-\frac{1}{5}\right\},\{0,0,0,0,0\},\left\{1,\frac{1}{2},\frac{1}{3},\frac{1}{4},\frac{1}{5}\right\},\left\{2,1,\frac{2}{3},\frac{1}{2},\frac{2}{5}\right\},\left\{3,\frac{3}{2},1,\frac{3}{4},\frac{3}{5}\right\},\left\{4,2,\frac{4}{3},1,\frac{4}{5}\right\},\left\{5,\frac{5}{2},\frac{5}{3},\frac{5}{4},1\right\}\right\}$$

```
Out[9]= {{62, 31, 43, 49, 66}, {63, 65, 21, 66, 26}, {64, 32, 66, 16, 53}, {65, 66, 44, 33, 13},
         {66, 33, 22, 50, 40}, {0, 0, 0, 0, 0}, {1, 34, 45, 17, 27}, {2, 1, 23, 34, 54}, {3, 35, 1, 51, 14}, {4, 2, 46, 1, 41}, {5, 36, 24, 18, 1}}

In[13]:= Length[Union[%8 // Flatten]]
         |长度   |并集        |压平
         Length[Union[%9 // Flatten]]
         |长度   |并集        |压平
Out[13]= 39

Out[14]= 39
```

欧几里得算法powerful

1.求两数GCD；
2.求整系数二元一次不定方程 （希尔伯特弱零点定理）；
3.有限域下求模逆；
4.求有理数的有限域原像；

Z_{67}

18 s + 67 t == r

s	t	r	Guess r/s	RatMod[r,s]
0	1	67	-	
1	0	18	18/1	18
-3	1	13	-13/3	18
4	-1	5	5/4	18
-11	3	3	-3/11	18
15	-4	2	2/15	18
-26	7	1	-1/26	18

欧几里得算法

$$
\begin{aligned}
r_0 &= a \\
s_0 &= 1 \\
t_0 &= 0 \\
r_1 &= b \\
s_1 &= 0 \\
t_1 &= 1 \\
\cdots &= \cdots \\
q_i &= \lfloor r_{i-2}/r_{i-1} \rfloor \\
r_i &= r_{i-2} - q_i\, r_{i-1} \\
s_i &= s_{i-2} - q_i\, s_{i-1} \\
t_i &= t_{i-2} - q_i\, t_{i-1}.
\end{aligned}
$$

```
RatRecByEuclid[num_, p_] := Module[{resR, resS},
                            模块
  r[0] = num; s[0] = 1; t[0] = 0;
  r[1] = p; s[1] = 0; t[1] = 1;
  i = 2;
  While[True,
  Whi…  真
   q[i] = IntegerPart[r[i - 2] / r[i - 1]];
          整数部分
   r[i] = r[i - 2] - q[i] r[i - 1];
   s[i] = s[i - 2] - q[i] s[i - 1];
   t[i] = t[i - 2] - q[i] t[i - 1];
   resR = r[i];
   resS = s[i];
   Print[{r[i] / s[i], t[i]}];
   打印
   If[2 r[i] r[i] < p && 2 s[i] s[i] < p, Break[]];
   如果                                   跳出循环
   If[r[i] == 1, Print["No preimage of ",
   如果          打印
     num, " in Z", p]; Break[]];
                       跳出循环
   i++];
  resR / resS]
```

In[24]:=
```
RatRecByEuclid[43, 67]
```

$\{43, 0\}$

$\{-24, 1\}$

$\left\{\frac{19}{2}, -1\right\}$

$\left\{-\frac{5}{3}, 2\right\}$

Out[24]= $-\frac{5}{3}$

In[25]:=
```
RatRecByEuclid[54, 67]
```

$\{54, 0\}$

$\{-13, 1\}$

$\left\{\frac{2}{5}, -4\right\}$

Out[25]= $\frac{2}{5}$

In[22]:=
```
RatRecByEuclid[6, 67]
```

$\{6, 0\}$

$\left\{-\frac{1}{11}, 1\right\}$

No image of 6 in Z67

Out[22]= $-\frac{1}{11}$

中国剩余定理

- If[2r[i]*r[i]<p,Break[]]?????

今有物不知其数，
三三数之剩二，
五五数之剩三，
七七数之剩二，
问物几何？

More in detail, given $a \in Z_n$, a set of pairwise co-prime numbers $n_1, \ldots n_k$ such that $n = n_1 \cdots n_k$, and a set of congruences

$$a_i = a \bmod n_i, \tag{A.9}$$

a can be uniquely determined in $\mathbb{Z}_n$ as

$$a = \sum_i m_i a_i \bmod n, \tag{A.10}$$

where

$$m_i \equiv \left(\left(\frac{n}{n_i} \right)^{-1} \bmod n_i \right) \frac{n}{n_i}. \tag{A.11}$$

中国剩余定理

```
In[26]:= Mod[46, 3]
         模余
         Mod[46, 5]
         模余
         Mod[46, 7]
         模余

Out[26]= 1

Out[27]= 1

Out[28]= 4
```

```
In[29]:= m1 = ModularInverse[105 / 5, 5] * 105 / 5
          模逆

Out[29]= 21

In[30]:= m2 = ModularInverse[105 / 7, 7] * 105 / 7
          模逆

Out[30]= 15

In[31]:= m3 = ModularInverse[105 / 3, 3] * 105 / 3
          模逆

Out[31]= 70

In[32]:= n = 3 * 5 * 7

Out[32]= 105

In[33]:= a = m1 * 1 + m2 * 4 + m3 * 1

Out[33]= 151

In[34]:= Mod[a, n]
         模余

Out[34]= 46
```

Outline

01 • 有理数重构

02 • 函数重构

03 • 应用

函数重构

- 单元多项式
- 单元有理函数

- 多元多项式
- 多元有理函数

问题引入：函数重构

```
In[63]:= aMat = Table[RandomInteger[20] a + i + j, {i, 2, 6}, {j, 2, 6}];
         |表格    |伪随机整数
         aMat // MatrixForm
                 |矩阵格式
         Inverse[aMat] // Simplify // MatrixForm
         |逆              |化简          |矩阵格式
         Table[Inverse[aMat], {i, 1, 1000}]; // Timing
         |表格    |逆                          |计算时间
```

Out[64]//MatrixForm=

$$\begin{pmatrix} 4+2a & 5+20a & 6+a & 7+6a & 8+10a \\ 5+11a & 6+a & 7+12a & 8+7a & 9+2a \\ 6+16a & 7+8a & 8+10a & 9+4a & 10+4a \\ 7+5a & 8+14a & 9+12a & 10+19a & 11+a \\ 8+7a & 9+3a & 10+19a & 11+3a & 12+17a \end{pmatrix}$$

$$\frac{2\left(-686+2693\,a+7075\,a^2\right)}{a\left(44\,156+173\,495\,a+117\,492\,a^2\right)}$$

Out[65]//MatrixForm=

$$\begin{pmatrix} \frac{2\left(-686+2693\,a+7075\,a^2\right)}{a\left(44\,156+173\,495\,a+117\,492\,a^2\right)} & \frac{-1674+19\,175\,a+37\,240\,a^2}{a\left(44\,156+173\,495\,a+117\,492\,a^2\right)} & \frac{5643+4611\,a-11\,555\,a^2}{44\,156\,a+173\,495\,a^2+117\,492\,a^3} & -\frac{8\left(97+1349\,a+1789\,a^2\right)}{a\left(44\,156+173\,495\,a+117\,492\,a^2\right)} & -\frac{1821+9736\,a+9144\,a^2}{44\,156\,a+173\,495\,a^2+117\,492\,a^3} \\ \frac{1680-15\,227\,a-15\,752\,a^2}{44\,156\,a+173\,495\,a^2+117\,492\,a^3} & -\frac{718+56\,106\,a+51\,088\,a^2}{44\,156\,a+173\,495\,a^2+117\,492\,a^3} & \frac{-2565+28\,743\,a+28\,598\,a^2}{a\left(44\,156+173\,495\,a+117\,492\,a^2\right)} & \frac{564+18\,623\,a+16\,580\,a^2}{44\,156\,a+173\,495\,a^2+117\,492\,a^3} & \frac{1039+9263\,a+7572\,a^2}{44\,156\,a+173\,495\,a^2+117\,492\,a^3} \\ \frac{868-35\,163\,a-31\,708\,a^2}{44\,156\,a+173\,495\,a^2+117\,492\,a^3} & \frac{4728-75\,708\,a-70\,496\,a^2}{44\,156\,a+173\,495\,a^2+117\,492\,a^3} & \frac{-8816+34\,317\,a+37\,144\,a^2}{a\left(44\,156+173\,495\,a+117\,492\,a^2\right)} & \frac{-24+28\,978\,a+25\,528\,a^2}{a\left(44\,156+173\,495\,a+117\,492\,a^2\right)} & \frac{4\left(811+5474\,a+4176\,a^2\right)}{a\left(44\,156+173\,495\,a+117\,492\,a^2\right)} \\ \frac{-1288+17\,407\,a+26\,450\,a^2}{a\left(44\,156+173\,495\,a+117\,492\,a^2\right)} & \frac{-606+51\,822\,a+69\,196\,a^2}{a\left(44\,156+173\,495\,a+117\,492\,a^2\right)} & \frac{2755-27\,273\,a-39\,659\,a^2}{44\,156\,a+173\,495\,a^2+117\,492\,a^3} & \frac{1460-10\,737\,a-17\,204\,a^2}{44\,156\,a+173\,495\,a^2+117\,492\,a^3} & -\frac{2321+14\,479\,a+13\,356\,a^2}{44\,156\,a+173\,495\,a^2+117\,492\,a^3} \\ \frac{112+20\,345\,a+27\,724\,a^2}{44\,156\,a+173\,495\,a^2+117\,492\,a^3} & \frac{5\left(-346+8231\,a+12\,052\,a^2\right)}{a\left(44\,156+173\,495\,a+117\,492\,a^2\right)} & \frac{2983-21\,835\,a-34\,804\,a^2}{44\,156\,a+173\,495\,a^2+117\,492\,a^3} & -\frac{8\left(153+2420\,a+2816\,a^2\right)}{a\left(44\,156+173\,495\,a+117\,492\,a^2\right)} & -\frac{141+5305\,a+6972\,a^2}{44\,156\,a+173\,495\,a^2+117\,492\,a^3} \end{pmatrix}$$

Out[66]= {1.85938, Null}

Newton法

$$f(z) = \sum_{r=0}^{R} a_r \prod_{i=0}^{r-1}(z - y_i)$$
$$= a_0 + (z - y_0)\Big(a_1 + (z - y_1)\Big(a_2 + (z - y_2)\big(\cdots + (z - y_{r-1})\, a_r\big)\Big)\Big). \qquad (3.5)$$

The coefficients a_r can be computed recursively by evaluating the function f at the values y_i as

$$a_0 = f(y_0)$$
$$a_1 = \frac{f(y_1) - a_0}{y_1 - y_0}$$
$$a_2 = \Big(\big(f(y_2) - a_0\big)\frac{1}{y_2 - y_0} - a_1\Big)\frac{1}{y_2 - y_1}$$
$$\cdots = \cdots$$
$$a_r = \left(\Big(\big(f(y_r) - a_0\big)\frac{1}{y_r - y_0} - a_1\Big)\frac{1}{y_r - y_1} - \cdots - a_{r-1}\right)\frac{1}{y_r - y_{r-1}}. \qquad (3.6)$$

Thiele 法

$$f(z) = a_0 + \cfrac{z - y_0}{a_1 + \cfrac{z - y_1}{a_2 + \cfrac{z - y_3}{\cdots + \cfrac{z - y_{r-1}}{a_N}}}}$$

$$= a_0 + (z - y_0)\left(a_1 + (z - y_1)\left(a_2 + (z - y_2)\left(\cdots + \frac{z - y_{N-1}}{a_N}\right)^{-1}\right)^{-1}\right)^{-1}, \quad (3.10)$$

$$\begin{aligned}
a_0 &= f(y_0) \\
a_1 &= \frac{y_1 - y_0}{f(y_1) - a_0} \\
a_2 &= \left((f(y_2) - a_0)^{-1}(y_2 - y_0) - a_1\right)^{-1}(y_2 - y_1) \\
\cdots &= \cdots \\
a_j &= \left(\left((f(y_j) - a_0)^{-1}(y_j - y_0) - a_1\right)^{-1}(y_j - y_1) - \cdots - a_{j-1}\right)^{-1}(y_j - y_{j-1}). \quad (3.11)
\end{aligned}$$

有理数域下重构

```
In[117]:= eva = Table[Inverse[aMat /. a → y[i]][[1, 1]], {i, 0, 1000}]; // Timing
          |表格    |逆                                                  |计算时间
Out[117]= {0.125, Null}
```

```
In[68]:= eva[[1 ;; 10]]
```

$$\text{Out[68]}= \left\{\frac{18164}{335143}, \frac{5500}{143519}, \frac{142136}{4866207}, \frac{61643}{2618008}, \frac{126436}{6414885}, \frac{135086}{7972257}, \frac{104240}{7015729}, \frac{89}{6728}, \frac{1193252}{100102167}, \frac{33352}{3074615}\right\}$$

```
In[69]:= a[0] = eva[[1]];
         n = 1;
         While[True,
         |Whi···  |真
          x = eva[[n + 1]];
          Do[x = (y[n] - y[i]) / (x - a[i]), {i, 0, n - 1}];
          |Do循环
          a[n] = x;

          funRc = a[n];
          Do[funRc = a[i] + (z - y[i]) / funRc, {i, n - 1, 0, -1}];
          |Do循环
          funRc // Print;
                   |打印
          If[eva[[n + 2]] === (funRc /. z → y[n + 1]), Print[n]; Break[]];
          |如果                                        |打印      |跳出循环
          n++]
         funRc // Simplify
                  |化简
```

$$\frac{18164}{335143} - \frac{763592616\ (-1+z)}{48099388217}$$

$$\frac{18164}{335143} + \frac{-1+z}{-\frac{48099388217}{763592616} - \frac{132602738652848383483\ (-2+z)}{7779843991953369000}}$$

$$\frac{18164}{335143} + \frac{-1+z}{-\frac{48099388217}{763592616} + \frac{-2+z}{\frac{7779843991953369000}{132602738652848383483} + \frac{376098819090182898459719976\ (-3+z)}{281899295385575720067957833149}}}$$

$$\text{Out[72]}= \frac{2\left(-686 + 2693\,z + 7075\,z^2\right)}{z\left(44156 + 173495\,z + 117492\,z^2\right)}$$

有限域下重构(1)

```
In[17]:= p = 9223372036854775643
Out[17]= 9223372036854775643

In[77]:= evaFF = RatMod[Numerator[#], Denominator[#], p] & /@ eva[[1 ;; 10]]
                 |分子              |分母
Out[77]= {9170559801663456372, 2051623331437313928, 2140326441454169722, 8706494860909142666,
  2855116881842794181, 8739440592779163129, 4704132991499695688, 5556231698182581106, 4937189323968731243, 2835292609691016202}

In[78]:= eva[[1 ;; 10]]
Out[78]= {18164/335143, 5500/143519, 142136/4866207, 61643/2618008, 126436/6414885, 135086/7972257, 104240/7015729, 89/6728, 1193252/100102167, 33352/3074615}

In[79]:= RatRecByEuclid[#, p] & /@ evaFF
Out[79]= {18164/335143, 5500/143519, 142136/4866207, 61643/2618008, 126436/6414885, 135086/7972257, 104240/7015729, 89/6728, 1193252/100102167, 33352/3074615}
```

```
In[105]:= a[0] = evaFF[[1]];
          n = 1;
          While[n < 7,
          |While循环
           x = evaFF[[n + 1]];
           Do[x = (y[n] - y[i]) / (x - a[i]), {i, 0, n - 1}];
           |Do循环
           a[n] = x;

           funRc = a[n];
           Do[funRc = a[i] + (z - y[i]) / funRc, {i, n - 1, 0, -1}];
           |Do循环
           funRc // Print;
                    |打印
           temp1 = RatMod0[evaFF[[n + 2]], p];
           temp2 = RatMod0[(funRc /. z → y[n + 1]), p];
           If[temp1 === temp2, Print[n]; Break[]];
           |如果                |打印      |跳出循环
           n++]
          funRc // Simplify
                   |化简

          9170559801663456372 - 7118936470226142444 (-1 + z)
Out[108]= (741178753044356501978472931389071999050259656878830773305724388870127878680932 - 850877417852
            270459891499799060945248406864589502087900649686916161865520607087495670646588 z^2 - 25468865
           (174797038409810269030129362329229637941511002776450219791602 - 226012620083873642905914088466
            72681399420343036297518018574717382914636075367213547849498 z^2 - 6712916699106688458607244668
```

有限域下重构(2)

Out[108]=
$$\frac{741\,178\,753\,044\,356\,501\,978\,472\,931\,389\,071\,999\,050\,259\,656\,878\,830\,773\,305\,724\,388\,870\,127\,878\,680\,932 - 850\,877\,417\,852\,635\,523\,601\,230\,753\,429\,273\,326\,807\,702\,597\,513\,269\,493\,782\,519\,226\,432\,854\,707\,769\,122\,z + 270\,459\,891\,499\,799\,060\,945\,248\,406\,864\,589\,502\,087\,900\,649\,686\,916\,161\,865\,520\,607\,087\,495\,670\,646\,588\,z^2 - 25\,468\,865\,390\,396\,853\,397\,394\,812\,612\,207\,549\,239\,189\,749\,095\,157\,735\,005\,695\,693\,289\,123\,536\,063\,838\,z^3}{174\,797\,038\,409\,810\,269\,030\,129\,362\,329\,229\,637\,941\,511\,002\,776\,450\,219\,791\,602 - 226\,012\,620\,083\,873\,642\,905\,914\,088\,460\,278\,695\,403\,577\,878\,119\,327\,337\,419\,463\,z + 72\,681\,399\,420\,343\,036\,297\,518\,018\,574\,717\,382\,914\,636\,075\,367\,213\,547\,849\,498\,z^2 - 6\,712\,916\,699\,106\,688\,458\,607\,244\,665\,535\,031\,138\,785\,248\,769\,179\,201\,408\,157\,z^3}$$

In[113]:=
```
numeCoelist = Mod[#, p] & /@ CoefficientList[Numerator[%108], z]
              |模余          |系数列表              |分子
```

Out[113]= {8 655 736 067 872 408 322, 5 576 185 570 913 052 960, 2 049 285 997 259 981 471, 0}

In[124]:=
```
numeCoelist1 = RatMod0[#, p] & /@ (numeCoelist / 5 657 061 155 427 006 064)
```

Out[124]= {6 146 965 130 459 333 672, 7 572 790 330 286 553 043, 3 695 113 944 468 724 095, 0}

In[125]:=
```
numeCoelist2 = RatRecByEuclid[#, p] & /@ numeCoelist1
```

Out[125]= $\left\{-\frac{49}{1577}, \frac{2693}{22\,078}, \frac{7075}{22\,078}, 0\right\}$

In[130]:=
```
denoCoelist = Mod[#, p] & /@ CoefficientList[Denominator[%108], z]
              |模余          |系数列表              |分母
```

Out[130]= {0, 5 657 061 155 427 006 064, 5 757 482 262 860 835 836, 2 627 420 215 444 341 021}

In[131]:=
```
denoCoelist1 = RatMod0[#, p] & /@ (denoCoelist / 5 657 061 155 427 006 064)
```

Out[131]= {0, 1, 1 030 830 260 935 735 075, 2 829 091 196 375 601 989}

In[134]:=
```
RatRecByEuclid[1 030 830 260 935 735 075, p]
```

Out[134]= $\frac{24\,785}{6308}$

In[135]:=
```
denoCoelist2 = RatRecByEuclid[#, p] & /@ denoCoelist1
```

Out[135]= $\left\{0, 1, \frac{24\,785}{6308}, \frac{29\,373}{11\,039}\right\}$

In[136]:=
```
(Plus @@ (numeCoelist2 * {1, z, z^2, z^3})) / (Plus @@ (denoCoelist2 * {1, z, z^2, z^3})) // Simplify
 |加                                           |加                                          |化简
```

Out[136]= $\frac{2\left(-686 + 2693\,z + 7075\,z^2\right)}{z\left(44\,156 + 173\,495\,z + 117\,492\,z^2\right)}$

多元多项式

$$f(z_1,\ldots,z_n)=\sum_{r=0}^{R}a_r(z_2,\ldots,z_n)\prod_{i=0}^{r-1}(z_1-y_i), \tag{3.12}$$

where, as before, the y_i are distinct elements of $\mathbb{F}$. The solutions for the coefficients a_r in Eq. (3.6) also apply to the multivariate case, with the following substitutions

$$f(y_j)\longrightarrow f(y_j,z_2,\ldots,z_n),\qquad a_j\longrightarrow a_j(z_2,\ldots,z_n). \tag{3.13}$$

多元有理函数

The method illustrated in ref. [26] consists in introducing an auxiliary variable t and defining a new function $h \in \mathbb{F}(t, \mathbf{z})$ as

$$h(t, \mathbf{z}) = f(t\,\mathbf{z}) = f(t\,z_1, \ldots, t\,z_n). \tag{3.16}$$

Using the canonical representation of f given by Eq. (2.7) and denoting the total degree of the numerator and the denominator of f by R and R' respectively, we get

$$h(t, \mathbf{z}) = \frac{\sum_{r=0}^{R} p_r(\mathbf{z})\, t^r}{1 + \sum_{r'=1}^{R'} q_{r'}(\mathbf{z})\, t^{r'}}, \tag{3.17}$$

where

$$p_r(\mathbf{z}) \equiv \sum_{|\alpha|=r} n_\alpha\, \mathbf{z}^\alpha, \qquad q_{r'}(\mathbf{z}) \equiv \sum_{|\beta|=r'} d_\beta\, \mathbf{z}^\beta. \tag{3.18}$$

are in turn obtained by reconstructing

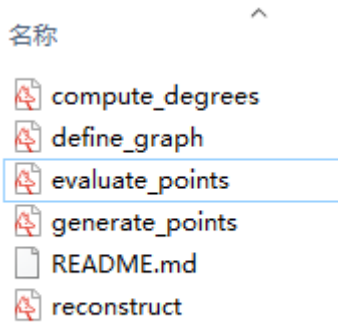
$$h_{\mathbf{y}_i}(t) \equiv h(t, \mathbf{y}_i) \tag{3.20}$$

as a univariate rational function in t and identifying $p_r(\mathbf{y}_i)$ and $q_{r'}(\mathbf{y}_i)$ with its coefficients.

Thank you!

Please comment ~~

利用Finiteflow重构函数



Machine-size number

degrees.fflow
points_3.fflow

evaluations_0_15_points_3.fflow

Address	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
00000000	05	00	00	00	00	00	00	00	03	00	00	00	00	00	00	00
00000010	0f	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000020	92	37	fa	12	9a	72	c4	6c	df	67	87	33	a0	b6	77	48
00000030	ef	6a	24	cb	fc	1a	70	49	e2	6e	cf	66	0e	3b	82	59
00000040	9d	f1	4c	bd	13	46	a8	48	d3	fe	ff	ff	ff	ff	ff	7f
00000050	03	00	00	00	00	00	00	00	30	d2	6e	7d	7e	4b	58	48
00000060	ec	d0	0e	67	40	6d	ef	10	d6	4c	1f	1e	ad	7d	0f	4c
00000070	26	48	c5	cc	7f	b1	ac	5f	71	06	54	71	1c	33	42	63
00000080	66	7a	09	b0	aa	06	8d	48	98	ac	eb	8a	f6	15	58	5c
00000090	e7	ff	ff	ff	ff	ff	ff	7f	03	00	00	00	00	00	00	00
000000a0	7d	37	03	c8	f8	55	1f	74	66	90	8a	99	ff	62	59	3f
000000b0	d6	4c	1f	1e	ad	7d	0f	4c	3c	65	a8	5d	10	0b	cf	26
000000c0	3a	06	7c	4b	c3	a3	68	33	12	9a	9f	31	54	2f	d6	06
000000d0	41	aa	ae	7a	9a	50	19	53	5b	ff	ff	ff	ff	ff	ff	7f
000000e0	02	00	00	00	00	00	00	00	79	ca	50	bb	20	16	9e	4d
000000f0	01	00	00	00	00	00	00	00	d6	4c	1f	1e	ad	7d	0f	4c
00000100	a7	4e	d4	c5	75	6d	47	63	9c	9f	04	c8	83	c3	89	70
00000110	91	cb	00	fa	50	c3	57	69	aa	13	18	77	a9	f0	c6	38
00000120	fd	fe	ff	ff	ff	ff	ff	7f	03	00	00	00	00	00	00	00
00000130	82	f3	74	95	a0	9c	09	61	52	9e	a8	8b	eb	da	8e	46
00000140	0b	69	fb	fd	af	7d	0f	4c	c1	9e	b8	42	1d	56	e9	05
00000150	39	9d	cf	f1	37	76	c7	20	4f	89	44	78	7e	bf	83	14
00000160	54	7e	a0	98	06	a7	bb	7b	fd	fe	ff	ff	ff	ff	ff	7f
00000170	03	00	00	00	00	00	00	00	3c	de	8a	ca	50	54	42	3c

https://github.com/peraro/finiteflow

T. Peraro, Scattering amplitudes over finite fields and multivariate functional reconstruction, JHEP 12 (2016) 030, [1608.01902].

进制的转换

```
In[*]:= list04 = Table[256^(i - 1), {i, 4}];
        |表格
        list08 = Table[256^(i - 1), {i, 8}];
        |表格
        Hexlist4ToDeci[exp_List] := Plus @@ (exp * list04);
                    |列表          |加
        Hexlist8ToDeci[exp_List] := Plus @@ (exp * list08);
                    |列表          |加
        HexlistToDecilist[exp_, num_Integer] := Module[{len, temp, list, res},
                                                |模块
          If[num =!= 4 && num =!= 8, Print["illegal input:", num]];
          |如果                     |打印
          len = Length[exp];
                |长度
          temp = QuotientRemainder[len, num];
                 |商和余数
          If[temp[[2]] =!= 0, Print["not complete"]];
          |如果               |打印
          list = Table[exp[[(num * i - num + 1) ;; (num * i)]], {i, 1, temp[[1]]}];
                 |表格
          Switch[num,
          |切换
           8, res = Hexlist8ToDeci /@ list,
           4, res = Hexlist4ToDeci /@ list];
          res
         ];
```

```
In[*]:= DeciToHexlist[exp_Integer] := Module[{list, temp},
                                      |模块
          list = {};
          If[exp === 0, Return[ConstantArray[0, 8]]]; (*faster*)
          |如果          |返回    |常量数组
          (*If[exp<256,Return[Join[{exp},ConstantArray[0,7]]]];*)
          temp = QuotientRemainder[exp, 256];
                 |商和余数
          AppendTo[list, temp[[2]]];
          |附加
          While[temp[[1]] =!= 0,
          |While循环
           temp = QuotientRemainder[temp[[1]], 256];
                  |商和余数
           AppendTo[list, temp[[2]]];
           |附加


          ];
          list = PadRight[list, 8];
                 |右填充
          (*While[Length[list]<8,AppendTo[list,0];];*)
          If[Length[list] > 8, Print["too large Integer:", exp]];
          |…  |长度              |打印
          list
         ];
```

FF特殊的文件格式

```
In[ ]:= listpoint = ReadList["points_1.fflow", Byte];
                    |读列表                    |字节
        sample = HexlistToDecilist[listpoint, 8];
        len = (Length[sample] - 2) / sample[[2]]
              |长度
Out[ ]= 5

In[ ]:= samp = Table[sample[[(len * (i - 1) + 3) ;; (len * i + 2)]], {i, sample[[2]]}];
              |表格
        Put[samp, "samp24.txt"]
        |写入
        flaglist = Table[Reverse[PadLeft[IntegerDigits[#, 2], 64, 0]] & /@ samp[[i, nparsin + 2 ;; len]] // Flatten, {i, sample[[2]]}];
                   |表格   |反向排序 |左填充   |不同进制的数字表示                                                  |压平
```

```
In[ ]:= evalist = Table[Join[samp[[i]], PadRight[solmicoeList[[i, Flatten[Position[flaglist[[i]], 1]]]], nparsout, 0]], {i, sample[[2]]}];
                  |表格   |连接              |右填充                    |压平      |位置
        evafflow = Join[{nparsin, nparsout + Ceiling[nparsout / 64], sample[[2]], 0}, evalist] // Flatten;
                   |连接                      |向上取整                                                |压平
        evafflowhexlist = DeciToHexlist /@ evafflow; // Timing
                                                     |计算时间
        BinaryWrite["evaluations_0_5473_points_1.fflow", evafflowhexlist]; // Timing
        |写字节                                                            |计算时间
```