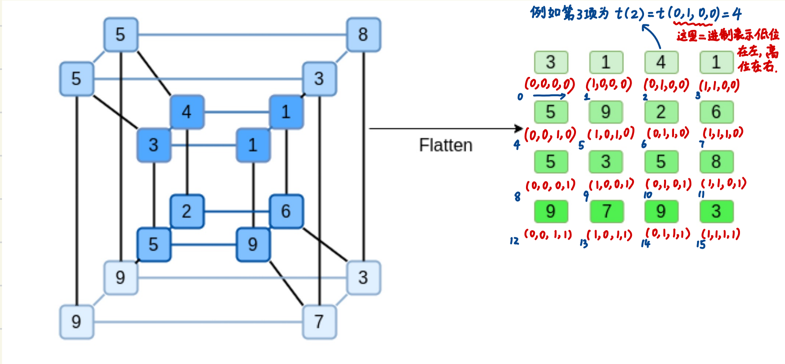
Binius: highly efficient proofs over binary fields

Jade Xie

Simple Binius – an example

Prover：承诺一个 multilinear polynomial $\tilde{t}(x_0,x_1,x_2,x_3)$ （x_i 不局限于 $\{0,1\}$，可取更多的值，其实这里进行了 MLE）



则 $t(0,0,0,0)=3$　　$t(0,0,1,0)=5$　　$t(0,0,0,1)=5$　　$t(0,0,1,1)=9$

$t(1,0,0,0)=1$　　$t(1,0,1,0)=9$　　$t(1,0,0,1)=3$　　$t(1,0,1,1)=7$

$t(0,1,0,0)=4$　　$t(0,1,1,0)=2$　　$t(0,1,0,1)=5$　　$t(0,1,1,1)=9$

$t(1,1,0,0)=1$　　$t(1,1,1,0)=6$　　$t(1,1,0,1)=8$　　$t(1,1,1,1)=3$

如何手算 $\tilde{t}(x_0,x_1,x_2,x_3)$ 呢？（在论文 Succinct Arguments over Towers of Binary Fields 2.1 Polynomials）

$$\tilde{t}(x_0,x_1,x_2,x_3)=\sum_{v\in B_v} t(v)\cdot \widetilde{eq}(v_0,v_1,v_2,v_3,x_0,x_1,x_2,x_3) \qquad B_v=\{0,1\}^4$$

$$\widetilde{eq}(v_0,v_1,v_2,v_3,x_0,x_1,x_2,x_3)=\prod_{i=0}^{3}\left(v_i\cdot x_i+(1-v_i)\cdot(1-x_i)\right)$$

其实也可以把这里看作选择器，$v_i=0$，选择 $(1-x_i)$

$v_i=1$，选择 x_i

连乘展开

当 $(v_0,v_1,v_2,v_3)=(0,0,0,0)$ 时，

$$\widetilde{eq}(v_0,v_1,v_2,v_3,x_0,x_1,x_2,x_3)=(v_0\cdot x_0+(1-v_0)\cdot(1-x_0))\cdot(v_1\cdot x_1+(1-v_1)\cdot(1-x_1))\cdot(v_2\cdot x_2+(1-v_2)\cdot(1-x_2))\cdot(v_3\cdot x_3+(1-v_3)\cdot(1-x_3))$$

$$=(1-x_0)(1-x_1)(1-x_2)(1-x_3)$$

代入 $v_0=0,\ v_1=0,\ v_2=0,\ v_3=0$

当 $(v_0,v_1,v_2,v_3)=(1,0,0,0)$ 时，

$$\widetilde{eq}(v_0,v_1,v_2,v_3,x_0,x_1,x_2,x_3)=x_0(1-x_1)(1-x_2)(1-x_3)$$

$\vdots$

当 $(v_0,v_1,v_2,v_3)=(1,1,1,1)$ 时，

$$\widetilde{eq}(v_0,v_1,v_2,v_3,x_0,x_1,x_2,x_3)=x_0x_1x_2x_3$$

现在代入 $\tilde{t}(x_0,x_1,x_2,x_3)$ 的计算

$$\tilde{t}(x_0,x_1,x_2,x_3)=\sum_{v\in B_v} t(v)\cdot \widetilde{eq}(v_0,v_1,v_2,v_3,x_0,x_1,x_2,x_3) \qquad B_v=\{0,1\}^4$$

$$\begin{aligned}
&=3(1-x_0)(1-x_1)(1-x_2)(1-x_3)+1\cdot x_0(1-x_1)(1-x_2)(1-x_3)+4\cdot(1-x_0)x_1(1-x_2)(1-x_3)+1\cdot x_0x_1(1-x_2)(1-x_3)\\
&+5\cdot(1-x_0)(1-x_1)x_2(1-x_3)+9\cdot x_0(1-x_1)x_2(1-x_3)+2\cdot(1-x_0)x_1x_2(1-x_3)+6\cdot x_0x_1x_2(1-x_3)\\
&+5\cdot(1-x_0)(1-x_1)(1-x_2)x_3+3\cdot x_0(1-x_1)(1-x_2)x_3+5\cdot(1-x_0)x_1(1-x_2)x_3+8\cdot x_0x_1(1-x_2)x_3\\
&+9\cdot(1-x_0)(1-x_1)x_2x_3+7\cdot x_0(1-x_1)x_2x_3+9\cdot(1-x_0)x_1x_2x_3+3\cdot x_0x_1x_2x_3
\end{aligned}$$

Prover 承诺 $\tilde{t}(r_0,r_1,r_2,r_3)=\tilde{t}(1,2,3,4)$ 的值，代入 $\tilde{t}(x_0,x_1,x_2,x_3)$ 可得

$$\begin{aligned}
\tilde{t}(1,2,3,4)&=3(1-1)(1-2)(1-3)(1-4)+1\cdot1\cdot(1-2)(1-3)(1-4)+4\cdot(1-1)\,2\,(1-3)(1-4)+1\cdot1\cdot2\cdot(1-3)(1-4)\\
&+5(1-1)(1-2)\cdot3\cdot(1-4)+9\cdot1\cdot(1-2)\cdot3\cdot(1-4)+2\cdot(1-1)\cdot2\cdot3\cdot(1-4)+6\cdot1\cdot2\cdot3\cdot(1-4)\\
&+5\cdot(1-1)(1-2)(1-3)\cdot4+3\cdot1\cdot(1-2)(1-3)\cdot4+5(1-1)\cdot2\cdot(1-3)\,4+8\cdot1\cdot2\cdot(1-3)\cdot4\\
&+9\cdot(1-1)(1-2)\cdot3\cdot4+7\cdot1\cdot(1-2)\cdot3\cdot4+9\cdot(1-1)\cdot2\cdot3\cdot4+3\cdot1\cdot2\cdot3\cdot4\\
&=0+(-6)+0+12\\
&+0+81+0+(-108)\\
&+0+24+0+(-128)\\
&+0+(-84)+0+72\\
&=6-27-104-12\\
&=-137
\end{aligned}$$

因此 Prover 承诺 $\tilde{f}(1,2,3,4) = -137$.

Prover 要对原来的方阵进行 Reed-Solomon code.

$x=$ 0	1	2	3		Extend	$x=$ 4	5	6	7
3	1	4	1	$f_1(x)$		-19	-67	-154	-291
5	9	2	6	$f_2(x)$	$\longrightarrow$	43	135	304	572
5	3	5	8	$f_3(x)$		9	5	-7	-30
9	7	9	3	$f_4(x)$		-23	-81	-183	-341

对于第1行，先用 Lagrange 插值算出 $f_1(x)$，满足

$$f_1(0) = 3 \quad a_0$$
$$f_1(1) = 1 \quad a_1$$
$$f_1(2) = 4 \quad a_2$$
$$f_1(3) = 1 \quad a_3$$

回顾下 Lagrange 插值公式

$$L_i(x) = \prod_{\substack{j=0 \\ j\neq i}}^{3} \frac{x-x_j}{x_i-x_j} \qquad \begin{matrix} x_0 = 0 \\ x_1 = 1 \\ x_2 = 2 \\ x_3 = 3 \end{matrix}$$

$$f_1(x) = a_0 L_0(x) + a_1 L_1(x) + a_2 L_2(x) + a_3 L_3(x)$$
$$= 3\times\frac{(x-1)(x-2)(x-3)}{(0-1)(0-2)(0-3)} + 1\times\frac{(x-0)(x-2)(x-3)}{(1-0)(1-2)(1-3)} + 4\times\frac{(x-0)(x-1)(x-3)}{(2-0)(2-1)(2-3)} + 1\times\frac{(x-0)(x-1)(x-2)}{(3-0)(3-1)(3-2)}$$
$$= -\frac{1}{2}(x-1)(x-2)(x-3) + \frac{1}{2}\times x(x-2)(x-3) - 2x(x-1)(x-3) + \frac{1}{6}x(x-1)(x-2)$$

因此，计算在 evaluation points 上的值 $X = \{4,5,6,7\}$

$$f_1(4) = -\frac{1}{2}\times3\times2\times1 + \frac{1}{2}\times4\times2\times1 - 2\times4\times3\times1 + \frac{1}{6}\times4\times3\times2 = -3+4-24+4 = -19$$
$$f_1(5) = -\frac{1}{2}\times4\times3\times2 + \frac{1}{2}\times5\times3\times2 - 2\times5\times4\times2 + \frac{1}{6}\times5\times4\times3 = -12+15-80+10 = -67$$
$$f_1(6) = -\frac{1}{2}\times5\times4\times3 + \frac{1}{2}\times6\times4\times3 - 2\times6\times5\times3 + \frac{1}{6}\times6\times5\times4 = -30+36-180+20 = -154$$
$$f_1(7) = -\frac{1}{2}\times6\times5\times4 + \frac{1}{2}\times7\times5\times4 - 2\times7\times6\times4 + \frac{1}{6}\times7\times6\times5 = -60+70-336+35 = -291$$

因此

$$3 \quad 1 \quad 4 \quad 1 \xrightarrow{\text{RS code}} -19 \quad -67 \quad -154 \quad -291$$

剩下第2, 3, 4行类似，先在 $x=\{0,1,2,3\}$ 上表示一个3次多项式 $f_i(x)$，再在点 $X=\{4,5,6,7\}$ 上计算值，得到 $f_i(4), f_i(5), f_i(6), f_i(7)$.

上述过程就是 Reed-Solomon 编码. 下面看看其一般的定义:

Essential Coding Theory Chapter 5.

Definition 5.2.1 (Reed-Solomon code). *Let $\mathbb{F}_q$ be a finite field, and choose n and k satisfying $k \le n \le q$. Fix a sequence $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots \alpha_n)$ of n distinct elements (also called* evaluation points*) from $\mathbb{F}_q$. We define an encoding function for Reed-Solomon code $\mathrm{RS}_q[\boldsymbol{\alpha}, k] : \mathbb{F}_q^k \to \mathbb{F}_q^n$ as follows. Map a message $\mathbf{m} = (m_0, m_1, \ldots, m_{k-1})$ with $m_i \in \mathbb{F}_q$ to the degree $k-1$ polynomial.*

$$\mathbf{m} \mapsto f_{\mathbf{m}}(X),$$

where

$$f_{\mathbf{m}}(X) = \sum_{i=0}^{k-1} m_i X^i. \qquad (5.1)$$

与这里有点区别，但本质相同

Note that $f_{\mathbf{m}}(X) \in \mathbb{F}_q[X]$ is a polynomial of degree at most $k-1$. The encoding of $\mathbf{m}$ is the evaluation of $f_{\mathbf{m}}(X)$ at all the α_i's :

$$\mathrm{RS}_q[\boldsymbol{\alpha}, k](\mathbf{m}) = \big(f_{\mathbf{m}}(\alpha_1), f_{\mathbf{m}}(\alpha_2), \ldots, f_{\mathbf{m}}(\alpha_n)\big).$$

When $q, \boldsymbol{\alpha}$ and k are known from context, we suppress them in the notation and simply refer to the map as RS. We call the image of this map, i.e., the set $\{\mathrm{RS}[\mathbf{m}] | \mathbf{m} \in \mathbb{F}_q^k\}$, the Reed-Solomon code or RS code. A common special case is $n = q-1$ with the set of evaluation points being $\mathbb{F}^* \stackrel{\text{def}}{=} \mathbb{F} \setminus \{0\}$.

对于 Reed-Solomon code，一个重要的性质是:

Claim 5.2.2. RS *codes are linear codes.*

Proof. The proof follows from the fact that if $a \in \mathbb{F}_q$ and $f(X), g(X) \in \mathbb{F}_q[X]$ are polynomials of degree $\le k-1$, then $af(X)$ and $f(X)+g(X)$ are also polynomials of degree $\le k-1$. In particular, let messages $\mathbf{m}_1$ and $\mathbf{m}_2$ be mapped to $f_{\mathbf{m}_1}(X)$ and $f_{\mathbf{m}_2}(X)$ where $f_{\mathbf{m}_1}(X), f_{\mathbf{m}_2}(X) \in \mathbb{F}_q[X]$ are polynomials of degree at most $k-1$ and because of the mapping defined in (5.1), it can be verified that:

$$f_{\mathbf{m}_1}(X) + f_{\mathbf{m}_2}(X) = f_{\mathbf{m}_1+\mathbf{m}_2}(X),$$

and

$$af_{\mathbf{m}_1}(X) = f_{a\mathbf{m}_1}(X).$$

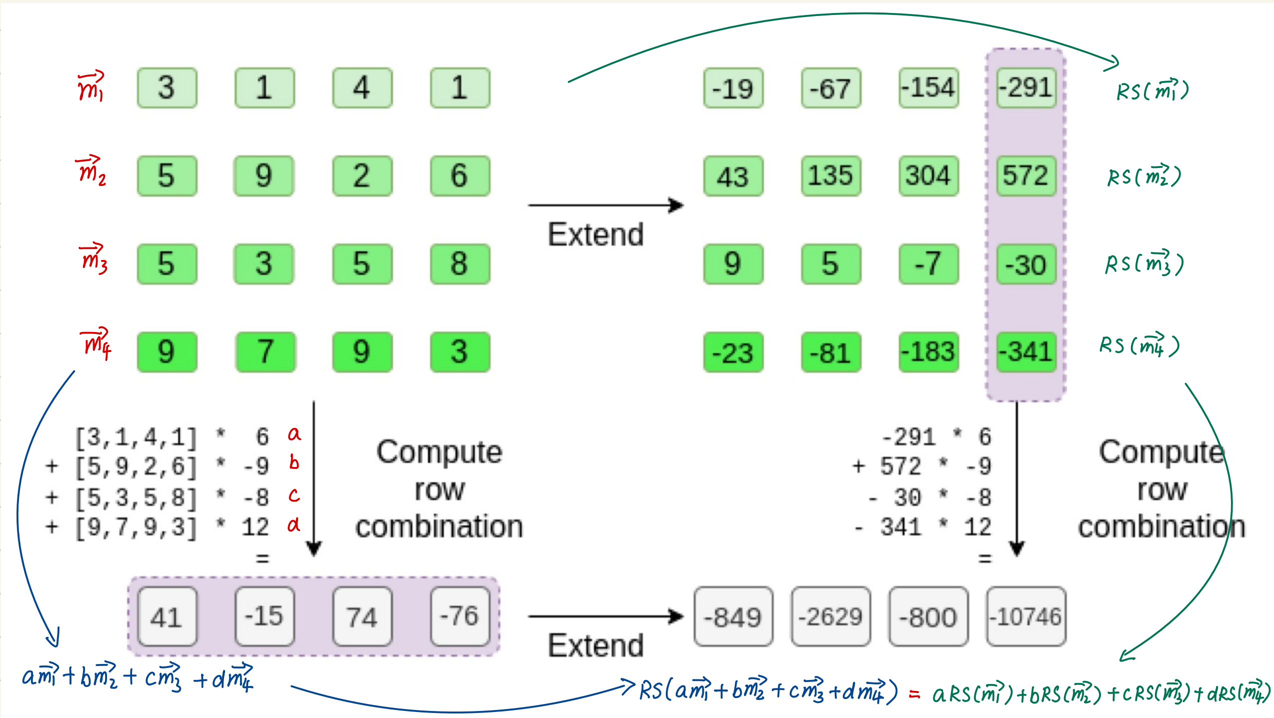
In other words,

$$\mathrm{RS}(\mathbf{m}_1) + \mathrm{RS}(\mathbf{m}_2) = \mathrm{RS}(\mathbf{m}_1 + \mathbf{m}_2)$$

$$a\mathrm{RS}(\mathbf{m}_1) = \mathrm{RS}(a\mathbf{m}_1).$$

Therefore RS is a $[n,k]_q$ linear code. □

因此有 $RS(a\vec{m_1} + b\vec{m_2}) = aRS(\vec{m_1}) + bRS(\vec{m_2})$



再来理解文中将 $r=\{1,2,3,4\}$ 分成两个部分，为什么分成两个部分计算后的值与开始代入一起算的值相同？均为-137.

↳ a linear combination of rows

a linear combination of columns with a row

这里引入了张量积的符号

$\bigotimes_{i=0}^{1}(1-r_i, r_i)$, $\bigotimes_{i=2}^{3}(1-r_i, r_i)$

它其实表示一个向量，在论文中的表述如下：

For each fixed $(r_0,\dots,r_{\nu-1}) \in K^\nu$, the vector $(\widetilde{\mathrm{eq}}(v_0,\dots,v_{\nu-1},r_0,\dots,r_{\nu-1}))_{v\in\mathcal{B}_\nu}$ takes the form

$$\left(\prod_{i=0}^{\nu-1} v_i \cdot r_i + (1-v_i)\cdot(1-r_i)\right)_{v\in\mathcal{B}_\nu} = ((1-r_0)\cdot\dots\cdot(1-r_{\nu-1}),\dots,r_0\cdot\dots\cdot r_{\nu-1}).$$

这里有 2^ν 个分量

We call this vector the *tensor product expansion* of the point $(r_0,\dots,r_{\nu-1}) \in K^\nu$, and denote it by $\bigotimes_{i=0}^{\nu-1}(1-r_i, r_i)$. We note the recursive description $\bigotimes_{i=0}^{\nu-1}(1-r_i,r_i) = (1-r_0)\cdot\bigotimes_{i=1}^{\nu-1}(1-r_i,r_i) \parallel r_0\cdot\bigotimes_{i=1}^{\nu-1}(1-r_i,r_i)$. This description yields a $\Theta(\nu)$-time algorithm which computes $\bigotimes_{i=0}^{\nu-1}(1-r_i,r_i)$ (see e.g. [Tha22, Lem. 3.8]).

对于我们要计算的 $\tilde{t}(r_0, r_1, r_2, r_3)$，对应论文中的 $\tilde{f}$

Each map $f \in K^{\mathcal{B}_\nu}$ admits a *unique* degree-1 multivariate extension $\widehat{f} \in K[X_0, \ldots, X_{\nu-1}]^{\preceq 1}$ (see [Tha22, Fact 3.5]). We thus refer freely to *the* degree-1 multivariate extension of f; we write $\widetilde{f}$ for this polynomial and call it f's *multilinear extension* (MLE). We recall the *equality indicator function* $\mathsf{eq} : \mathcal{B}_\nu \times \mathcal{B}_\nu \to \mathcal{B}_\nu, (x, y) \mapsto x \stackrel{?}{=} y$, as well as its MLE, the *equality indicator polynomial* (see [Tha22, Lem. 3.6]):

$$\widetilde{\mathsf{eq}}(X_0, \ldots, X_{\nu-1}, Y_0, \ldots, Y_{\nu-1}) = \prod_{i=0}^{\nu-1} X_i \cdot Y_i + (1 - X_i) \cdot (1 - Y_i).$$

For each $f \in K^{\mathcal{B}_\nu}$, we have the following explicit representation of f's multilinear extension $\widetilde{f} \in K[X_0, \ldots, X_{\nu-1}]^{\preceq 1}$:

$$\widetilde{f}(X_0, \ldots, X_{\nu-1}) = \sum_{v \in \mathcal{B}_\nu} f(v) \cdot \widetilde{\mathsf{eq}}(v_0, \ldots, v_{\nu-1}, X_0, \ldots, X_{\nu-1}).$$

这里计算 $\tilde{f}(x_0, \cdots, x_{\nu-1})$ 也可这样计算：

向量 $\vec{a} = (f(v_0),\ f(v_1),\ \cdots,\ f(v_{2^\nu-1}))$

向量 $\vec{b} = \bigotimes_{i=0}^{\nu-1} (1-x_i, x_i)$

$= ((1-x_0)\cdots(1-x_{\nu-1}),\ \ldots,\ x_0\cdot\cdots\cdot x_{\nu-1})$

将 $\vec{a}, \vec{b}$ 向量的分量分别相乘再相加，即得 $\tilde{f}(x_0, \cdots, x_{\nu-1})$，即

$\tilde{f}(x_0, \cdots, x_{\nu-1}) = \vec{a} \cdot \vec{b}^T$

对于本文中的 $\tilde{t}(r_0, r_1, r_2, r_3) = \tilde{t}(1, 2, 3, 4)$

$\vec{a} = (f(v_0), f(v_1), \cdots, f(v_{2^4-1}))$

$= (3, 1, 4, 1, 5, 9, 2, 6, 5, 3, 5, 8, 9, 7, 9, 3)$

$\vec{b} = \bigotimes_{i=0}^{3} (1-r_i, r_i)$

$= ((1-r_0)(1-r_1)(1-r_2)(1-r_3),\ \ldots,\ r_0 r_1 r_2 r_3)$

对应分量相乘再相加

对比之前我们的计算方式，是一致的

$\tilde{t}(r_0, r_1, r_2, r_3) = \vec{a} \cdot \vec{b}^T$

$\tilde{t}(1,2,3,4) = 3(1-1)(1-2)(1-3)(1-4) + 1\cdot 1\cdot(1-2)(1-3)(1-4) + 4\cdot(1-1)\,2\,(1-3)(1-4) + 1\cdot 1\cdot 2\cdot(1-3)(1-4)$
$+ 5(1-1)(1-2)\cdot 3\cdot(1-4) + 9\cdot 1\cdot(1-2)\cdot 3\cdot(1-4) + 2\cdot(1-1)\cdot 2\cdot 3\cdot(1-4) + 6\cdot 1\cdot 2\cdot 3\cdot(1-4)$
$+ 5\cdot(1-1)(1-2)(1-3)\cdot 4 + 3\cdot 1\cdot(1-2)(1-3)\cdot 4 + 5(1-1)\cdot 2\cdot(1-3)\,4 + 8\cdot 1\cdot 2\cdot(1-3)\cdot 4$
$+ 9\cdot(1-1)(1-2)\cdot 3\cdot 4 + 7\cdot 1\cdot(1-2)\cdot 3\cdot 4 + 9\cdot(1-1)\cdot 2\cdot 3\cdot 4 + 3\cdot 1\cdot 2\cdot 3\cdot 4$
$= 0 + (-6) + 0 + 12$
$+ 0 + 81 + 0 + (-108)$
$+ 0 + 24 + 0 + (-128)$
$+ 0 + (-84) + 0 + 72$
$= 6 - 27 - 104 - 12$
$= -137$

现在把 $\vec{a}$ 和 $\vec{b}$ 分组一下

$\vec{a} = (\underbrace{[3, 1, 4, 1]}_{\vec{a_0}},\ \underbrace{[5, 9, 2, 6]}_{\vec{a_1}},\ \underbrace{[5, 3, 5, 8]}_{\vec{a_2}},\ \underbrace{[9, 7, 9, 3]}_{\vec{a_3}})$

$\vec{b} = \bigotimes_{i=0}^{3} (1-r_i, r_i)$

$= (1-r_0)(1-r_1)\cdot\bigotimes_{i=2}^{3}(1-r_i, r_i) \,\|\, (1-r_0)r_1\cdot\bigotimes_{i=2}^{3}(1-r_i, r_i) \,\|$
$r_0(1-r_1)\cdot\bigotimes_{i=2}^{3}(1-r_i, r_i) \,\|\, r_0 r_1\cdot\bigotimes_{i=2}^{3}(1-r_i, r_i)$

$= ((1-r_0)(1-r_1)[(1-r_2)(1-r_3), (1-r_2)r_3, r_2(1-r_3), r_2 r_3],$
$(1-r_0)r_1\,[(1-r_2)(1-r_3), (1-r_2)r_3, r_2(1-r_3), r_2 r_3],$
$r_0(1-r_1)\,[(1-r_2)(1-r_3), (1-r_2)r_3, r_2(1-r_3), r_2 r_3],$
$r_0 r_1\,[(1-r_2)(1-r_3), (1-r_2)r_3, r_2(1-r_3), r_2 r_3])$

先计算 $(\vec{a_0}, \vec{a_1}, \vec{a_2}, \vec{a_3}) \cdot (\bigotimes_{i=2}^{3}(1-r_i, r_i))^T$

再计算 $(\underbrace{(\vec{a_0}, \vec{a_1}, \vec{a_2}, \vec{a_3})}_{1\times 4} \cdot \underbrace{(\bigotimes_{i=2}^{3}(1-r_i, r_i))^T}_{4\times 1})_{1\times 4} \cdot \underbrace{(\bigotimes_{i=0}^{1}(1-r_i, r_i))^T}_{4\times 1}$ 1×1

因此

So here is how we do that check. We take the tensor product of what we labelled as the "column part" of the evaluation point:

$$\bigotimes_{i=0}^{1}(1 - r_i, r_i)$$

In our example, where $r = \{1, 2, 3, 4\}$ (so the half that chooses the column is $\{1, 2\}$), this equals:

$$[(1-1)*(1-2), 1*(1-2), (1-1)*2, 1*2] = [0, -1, 0, 2]$$

So now we take this linear combination of t':

$$0 * 41 + (-1) * (-15) + 0 * 74 + 2 * (-76) = -137$$

Which exactly equals the answer you get if you evaluate the polynomial directly.