多値論理多項式に対する離散フーリエ変換の応用と積の高速化

松井　一

豊田工業大学

IT・ISEC・WBS 合同研究会，2018 年 3 月 8 日 17:00-17:50

Contents[1]

[1] H. Matsui, "A convolution theorem for multiple-valued logic polynomials of a semigroup type and their fast multiplication," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol.E99-A, no.6, pp.1025–1033, Jun. 2016.

Background

A logic function means

$$F : (\mathbb{F}_2)^n \to \mathbb{F}_2, \quad \text{where } \mathbb{F}_2 \text{ is 2-element finite field} \quad \mathbb{F}_2 = \{0, 1\}.$$

Example (A logic function)

$$F : (\mathbb{F}_2)^2 \to \mathbb{F}_2,$$

x_1	x_2	$F(x_1, x_2)$
0	0	0
1	0	1
0	1	1
1	1	1

Such functions are used in (3-)SAT, Boolean algebra, digital electronic circuits, etc.

Example (A logic polynomial)

The above F is equal to a polynomial $F(x_1, x_2) = x_1 + x_2 + x_1 x_2 \in \mathbb{F}_2[x_1, x_2]$.

Background

Let n be a positive integer, q a prime power, $\mathbb{F}_q$ a finite field, and

$$F : \left(\mathbb{F}_q\right)^n \to \mathbb{F}_q \quad \begin{cases} \text{a logic function } (q = 2) \\ \text{a multiple-valued logic function } (q \geq 2). \end{cases}$$

Fact. we can construct a polynomial (Reed–Muller expansion)

$$f = f(x_1, \cdots, x_n) = \sum_{a_1=0}^{q-1} \cdots \sum_{a_n=0}^{q-1} f_{(a_1,\cdots,a_n)} x_1^{a_1} \cdots x_n^{a_n} \quad \text{with } f_{(a_1,\cdots,a_n)} \in \mathbb{F}_q$$

such that $f(\omega_1, \cdots, \omega_n) = F(\omega_1, \cdots, \omega_n)$ for all $(\omega_1, \cdots, \omega_n) \in \left(\mathbb{F}_q\right)^n$.

$$\text{(Computational complexity of } F \mapsto f) = \mathrm{O}\left(nq^{n+1}\right)$$

outperforms (Matrix-manipulation of size q^n) $= \mathrm{O}\left(q^{2n}\right)$.

Motivation

- On the other hand, for an arbitrary subset of $\left(\mathbb{F}_q\right)^n$, such low-complexity construction from F to f is not known.
- Only exception is the case of the product of cyclic subgroups with multiplicative operation $*$ in $\mathbb{F}_q$ (DFT case):

$$F : C_n \to \mathbb{F}_q \text{ where } C_n = \left\{(\omega_1, \cdots, \omega_n) \in \left(\mathbb{F}_q\right)^n \,\middle|\, \omega_i^{d_i} = 1\right\},\ d_i \mid (q-1).$$

- However, such cyclic subgroups do not contain zero element $0 \in \mathbb{F}_q$ and are not suitable for logic use.

$\Longrightarrow$ Subset "of a semigroup type":

$$F : \Omega_n \to \mathbb{F}_q \text{ where } \Omega_n = \left\{(\omega_1, \cdots, \omega_n) \in \left(\mathbb{F}_q\right)^n \,\middle|\, \omega_i^{d_i+1} = \omega_i\right\},\ d_i \mid (q-1).$$

Main results

For any function $F : \Omega_n \to \mathbb{F}_q$, we can construct a polynomial

$$f = f(x_1, \cdots, x_n) = \sum_{a_1=0}^{d_1} \cdots \sum_{a_n=0}^{d_n} f_{(a_1,\cdots,a_n)} x_1^{a_1} \cdots x_n^{a_n} \quad \text{with } f_{(a_1,\cdots,a_n)} \in \mathbb{F}_q$$

such that $f(\omega_1, \cdots, \omega_n) = F(\omega_1, \cdots, \omega_n)$ for all $(\omega_1, \cdots, \omega_n) \in \Omega_n$.

$$\text{(Computational complexity of } F \mapsto f) = \mathrm{O}\left(\left(\sum_{i=1}^{n}(d_i+1)\right)\prod_{i=1}^{n}(d_i+1)\right)$$

outperforms (Matrix-manipulation of size $\prod_{i=1}^{n}(d_i+1)) = \mathrm{O}\left(\prod_{i=1}^{n}(d_i+1)^2\right)$.

If $d_i + 1 = q$ for all i, then $\left(\sum_{i=1}^{n}(d_i+1)\right)\prod_{i=1}^{n}(d_i+1) = nq^{n+1}$.

Remarks

- This construction $F \mapsto f$ is applied to a fast multiplication algorithm for the multiple-valued logic polynomials.
- This algorithm is based on a convolution theorem.

- Cf. the convolution theorem of continuous Fourier transform

$$\mathcal{F}\left(\int f(\tau)g(t-\tau)d\tau\right) = \mathcal{F}(f)\mathcal{F}(g)$$

- Cf. FFT-based fast integer multiplication algorithms, where complex or modular arithmetic is used instead of finite-field arithmetic.

- Multiplication using Gröbner bases is equal to naïve multiplication.

Preliminaries

We define a quotient ring

$$R_n = \frac{\mathbb{F}_q[x_1, \cdots, x_n]}{\left(x_1^{d_1+1} - x_1, \cdots, x_n^{d_n+1} - x_n\right)},$$

where $\mathbb{F}_q[x_1, \cdots, x_n]$ denotes the n-variable polynomial ring with coefficients in $\mathbb{F}_q$, and $\left(x_1^{d_1+1} - x_1, \cdots, x_n^{d_n+1} - x_n\right)$ denotes an ideal in $\mathbb{F}_q[x_1, \cdots, x_n]$ generated by $x_1^{d_1+1} - x_1, \cdots, x_n^{d_n+1} - x_n$.

Then any monomial $x_1^{a_1} \cdots x_n^{a_n} \in R_n$ can be uniquely written by

$$(a_1, \cdots, a_n) \in A_n = \{a = (a_1, \cdots, a_n) \,|\, a_i = 0, 1, \cdots, d_i\}.$$

Moreover, any $f = f(x_1, \cdots, x_n) \in R_n$ can be uniquely written by

$$f = \sum_{a \in A_n} f_a x^a, \quad \text{where } x^a = x_1^{a_1} \cdots x_n^{a_n} \text{ for } a = (a_1, \cdots, a_n) \in A_n.$$

Example (Multiple-valued logic polynomials)

If $n = 1$, $q = 7$, and $d_1 = 3$, then an example of $f \in R_1$ is

$$f = f(x_1) = 2 + 1x_1 + 6x_1^2 + 5x_1^3.$$

If $n = 2$, $q = 7$, $d_1 = 2$, and $d_2 = 3$, then an example of $f \in R_2$ is

$$\begin{aligned} f = f(x_1, x_2) = \; & 4 + 6x_2 + 5x_2^2 + 2x_2^3 \\ & + 1x_1 + 4x_1x_2 + 0x_1x_2^2 + 5x_1x_2^3 \\ & + 3x_1^2 + 5x_1^2x_2 + 1x_1^2x_2^2 + 4x_1^2x_2^3. \end{aligned}$$

Contents

Evaluation map ev_n

Let $\beta_i \in \mathbb{F}_q$ be a primitive d_i-th root of unity.
Then define a map $\mathrm{ev}_n : R_n \to R_n$, for $f = f(x_1, \cdots, x_n) \in R_n$, by

$$\mathrm{ev}_n(f) = \sum_{(a_1,\cdots,a_n)\in A_n} f\left(\beta_1^{\langle a_1\rangle}, \cdots, \beta_n^{\langle a_n\rangle}\right) x_1^{a_1} \cdots x_n^{a_n}, \text{ where } \beta_i^{\langle a_i\rangle} = \begin{cases} 0 & a_i = 0 \\ \beta_i^{a_i} & a_i \neq 0. \end{cases}$$

$$\text{(Computational complexity of } f\left(\beta_1^{\langle a_1\rangle}, \cdots, \beta_n^{\langle a_n\rangle}\right)) = 3\prod_{i=1}^{n}(d_i+1)$$

because

- updating of the value $\left(\beta_1^{\langle a_1\rangle}\right)^{b_1} \cdots \left(\beta_n^{\langle a_n\rangle}\right)^{b_n}$
- product with f_b
- addition to the sum
- these are done $|A_n| = \prod_{i=1}^{n}(d_i+1)$ times.

Thus (Computational complexity of $\mathrm{ev}_n(f)) = 3\prod_{i=1}^{n}(d_i+1)^2$.

Example (ev_1 and ev_2)

If $n = 1$, $q = 7$, and $d_1 = 3$, then we can set $\beta_1 = 2$, and $\mathrm{ev}_1(f) \in R_1$ for $f = 2 + 1x_1 + 6x_1^2 + 5x_1^3$ is equal to

$$\mathrm{ev}_1(f) = \mathrm{ev}_1(f)(x_1) = 2 + 5x_1 + 2x_1^2 + 0x_1^3.$$

If $n = 2$, $q = 7$, and $(d_1, d_2) = (2, 3)$, then we can set $(\beta_1, \beta_2) = (6, 2)$, and $\mathrm{ev}_2(f) \in R_2$ for f is equal to

$$\begin{array}{l} f = 4 \quad +6x_2 \quad +5x_2^2 \quad +2x_2^3 \\ \quad +1x_1 \ +4x_1x_2 \ +0x_1x_2^2 \ +5x_1x_2^3 \\ \quad +3x_1^2 \ +5x_1^2x_2 \ +1x_1^2x_2^2 \ +4x_1^2x_2^3. \end{array} \mapsto \begin{array}{l} \mathrm{ev}_2(f) = 4 \quad +3x_2 \quad +5x_2^2 \quad +3x_2^3 \\ \quad +6x_1 \ +3x_1x_2 \ +5x_1x_2^2 \ +6x_1x_2^3 \\ \quad +1x_1^2 \ +3x_1^2x_2 \ +0x_1^2x_2^2 \ +5x_1^2x_2^3. \end{array}$$

A convolution theorem

For $f = \sum_{a \in A_n} f_a x^a \in R_n$ and $g = \sum_{a \in A_n} g_a x^a \in R_n$, define

$$F_*(f, g) = fg \in R_n \quad \text{and} \quad F_\odot(f, g) = \sum_{a \in A_n} f_a g_a x^a \in R_n.$$

Then, $\mathrm{ev}_n \circ F_* = F_\odot \circ (\mathrm{ev}_n \times \mathrm{ev}_n)$, i.e., commutative diagram

$$\begin{array}{ccc} R_n \times R_n & \xrightarrow{\mathrm{ev}_n \times \mathrm{ev}_n} & R_n \times R_n \\ {\scriptstyle F_*}\downarrow & & \downarrow{\scriptstyle F_\odot} \\ R_n & \xrightarrow[\mathrm{ev}_n]{} & R_n. \end{array}$$

In other words, ev_n is a ring-homomorphism.

It is sufficient to prove only for monomials.

Contents

Recursive structure of ev_n

For non-empty subset $K = \{i_1, \cdots, i_k\} \subseteq \{1, \cdots, n\}$ with $k = |K|$, define an $\mathbb{F}_q$-linear map $\mathrm{ev}_{n,K} : R_n \to R_n$ by

$$\mathrm{ev}_{n,K}(f) = \sum_{(a_{i_1},\cdots,a_{i_k}) \in A_k} \left\{ f\Big|_{x_{i_1} = \beta_{i_1}^{\langle a_{i_1} \rangle}, \cdots, x_{i_k} = \beta_{i_k}^{\langle a_{i_k} \rangle}} \right\} \prod_{l=1}^{k} x_{i_l}^{a_{i_l}},$$

where $f = f(x_1, \cdots, x_n) \in R_n$. In particular, we have $\mathrm{ev}_n = \mathrm{ev}_{n,\{1,\cdots,n\}}$.

$$\Longrightarrow \quad \mathrm{ev}_{n,\{1,\cdots,l\}} = \mathrm{ev}_{n,\{l\}} \circ \mathrm{ev}_{n,\{1,\cdots,l-1\}} = \mathrm{ev}_{n,\{1,\cdots,l-1\}} \circ \mathrm{ev}_{n,\{l\}}$$

$$\Longrightarrow \quad \mathrm{ev}_n = \mathrm{ev}_{n,\{n\}} \circ \cdots \circ \mathrm{ev}_{n,\{2\}} \circ \mathrm{ev}_{n,\{1\}}$$

$$\Longrightarrow (\text{Computational complexity of } \mathrm{ev}_n(f)) = \mathrm{O}\left(\left(\sum_{i=1}^{n}(d_i+1)\right)\prod_{i=1}^{n}(d_i+1)\right)$$

Recursive structure of ev_n

We prove recursive structure of ev_n for $n = 2$. For $f = f(x_1, x_2) \in R_2$,

$$\begin{aligned}
\mathrm{ev}_{2,\{2\}}\left(\mathrm{ev}_{2,\{1\}}(f)\right) &= \mathrm{ev}_{2,\{2\}}\left(\sum_{a_1=0}^{d_1} f\left(\beta_1^{\langle a_1\rangle}, x_2\right) x_1^{a_1}\right) \\
&= \sum_{a_1=0}^{d_1} \mathrm{ev}_{2,\{2\}}\left(f\left(\beta_1^{\langle a_1\rangle}, x_2\right)\right) x_1^{a_1} \\
&= \sum_{a_1=0}^{d_1}\left(\sum_{a_2=0}^{d_2} f\left(\beta_1^{\langle a_1\rangle}, \beta_2^{\langle a_2\rangle}\right) x_2^{a_2}\right) x_1^{a_1} \\
&= \mathrm{ev}_{2,\{1,2\}}(f) = \mathrm{ev}_{2,\{1\}}\left(\mathrm{ev}_{2,\{2\}}(f)\right).
\end{aligned}$$

Cf. tensor product $\dfrac{\mathbb{F}_q[x_1, x_2]}{\left(x_1^{d_1+1} - x_1, x_2^{d_2+1} - x_2\right)} = \dfrac{\mathbb{F}_q[x_1]}{\left(x_1^{d_1+1} - x_1\right)} \bigotimes \dfrac{\mathbb{F}_q[x_2]}{\left(x_2^{d_2+1} - x_2\right)}$.

Example ($\mathrm{ev}_{1,\{1\}}$ and $\mathrm{ev}_{1,\{2\}}$)

Let $q = 7$, $(d_1, d_2) = (2, 3)$, $(\beta_1, \beta_2) = (6, 2)$.

For $f = \sum_{i=0}^{2} f_i x_1^i \in \dfrac{\mathbb{F}_q[x_1]}{(x_1^3 - x_1)}$, $\quad g = \sum_{i=0}^{3} g_i x_2^i \in \dfrac{\mathbb{F}_q[x_2]}{(x_2^4 - x_2)}$,

$$\mathrm{ev}_{1,\{1\}}(f) = \sum_{i=0}^{2} c_i x_1^i, \quad (c_0, c_1, c_2) = (f_0, f_1, f_2) M_1,$$

$$\mathrm{ev}_{1,\{2\}}(g) = \sum_{i=0}^{3} e_i x_2^i, \quad (e_0, e_1, e_2, e_3) = (g_0, g_1, g_2, g_3) M_2,$$

where

$$M_1 = \begin{array}{c} \\ 1 \\ x \\ x^2 \end{array} \begin{array}{c} \begin{array}{ccc} 0 & 6 & 1 \end{array} \\ \begin{pmatrix} 1 & 1 & 1 \\ 0 & 6 & 1 \\ 0 & 1 & 1 \end{pmatrix} \end{array}, \quad M_2 = \begin{array}{c} \\ 1 \\ x \\ x^2 \\ x^3 \end{array} \begin{array}{c} \begin{array}{cccc} 0 & 2 & 4 & 1 \end{array} \\ \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 2 & 4 & 1 \\ 0 & 4 & 2 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix} \end{array}.$$

Example ($\mathrm{ev}_{2,\{2\}} \circ \mathrm{ev}_{2,\{1\}} = \mathrm{ev}_2$)

$$M_1^\top = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 6 & 1 \\ 1 & 1 & 1 \end{pmatrix} \curvearrowright$$

$$\begin{aligned} R_2 \ni f = {} & 4 + 6x_2 + 5x_2^2 + 2x_2^3 \\ & + 1x_1 + 4x_1x_2 + 0x_1x_2^2 + 5x_1x_2^3 \\ & + 3x_1^2 + 5x_1^2x_2 + 1x_1^2x_2^2 + 4x_1^2x_2^3 \end{aligned}$$

$$\begin{aligned} \mathrm{ev}_{2,\{1\}}(f) = {} & 4 + 6x_2 + 5x_2^2 + 2x_2^3 \\ & + 6x_1 + 0x_1x_2 + 6x_1x_2^2 + 1x_1x_2^3 \\ & + 1x_1^2 + 1x_1^2x_2 + 6x_1^2x_2^2 + 4x_1^2x_2^3 \end{aligned} \curvearrowleft M_2 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 2 & 4 & 1 \\ 0 & 4 & 2 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

$$\begin{aligned} \mathrm{ev}_{2,\{2\}}(\mathrm{ev}_{2,\{1\}}(f)) = {} & 4 + 3x_2 + 5x_2^2 + 3x_2^3 \\ & + 6x_1 + 3x_1x_2 + 5x_1x_2^2 + 6x_1x_2^3 \\ & + 1x_1^2 + 3x_1^2x_2 + 0x_1^2x_2^2 + 5x_1^2x_2^3 \end{aligned}$$

$$\therefore \ \mathrm{ev}_{2,\{2\}}(\mathrm{ev}_{2,\{1\}}(f)) = \mathrm{ev}_2(f) = \mathrm{ev}_{2,\{1\}}(\mathrm{ev}_{2,\{2\}}(f))$$

Contents

Inverse transform ev_n^{-1}

It is sufficient to compute $\mathrm{ev}_{1,\{1\}}^{-1} = \mathrm{ev}_1^{-1}$ because

$$\mathrm{ev}_n = \mathrm{ev}_{n,\{n\}} \circ \cdots \circ \mathrm{ev}_{n,\{2\}} \circ \mathrm{ev}_{n,\{1\}} \Longrightarrow \mathrm{ev}_n^{-1} = \mathrm{ev}_{n,\{1\}}^{-1} \circ \cdots \circ \mathrm{ev}_{n,\{n-1\}}^{-1} \circ \mathrm{ev}_{n,\{n\}}^{-1},$$

$$\mathrm{ev}_{n,\{i\}}^{-1}(f) = \sum_{(a_1,\cdots,a_{i-1},a_{i+1},\cdots,a_n)} \mathrm{ev}_{1,\{i\}}^{-1}\left(\sum_{a_i=0}^{d_i} f_{(a_1,\cdots,a_n)} x_i^{a_i}\right) x_1^{a_1} \cdots x_{i-1}^{a_{i-1}} x_{i+1}^{a_{i+1}} \cdots x_n^{a_n}.$$

$\mathrm{ev}_1 : R_1 \to R_1$ is equal to $\mathrm{ev}_1(f) = \sum_{(a_1)\in A_1} f\left(\beta_1^{\langle a_1 \rangle}\right) x_1^{a_1}$.

Formula for ev_1^{-1}

$$\mathrm{ev}_1^{-1}(f) = f(0)\left(1 - x_1^{d_1}\right) + \frac{1}{d_1}\sum_{j=1}^{d_1}\left\{f\left(\beta_1^{-j}\right) - f(0)\right\} x_1^j.$$

We will prove this by Chinese remainder theorem.[2]

[2] H. Matsui, "On multiple-valued logic polynomials of a subset type", Recent Results Posters at ISITA2016, p.547, Monterey, California, October 30–November 2, 2016.

Another commutative diagram

$$A = \{0\}, \quad \mathrm{ev}_A : \frac{\mathbb{F}_q[x]}{(x)} \ni f_0 \mapsto f_0,$$

$$B = \left\{1, \beta, \cdots, \beta^{d-1}\right\}, \quad \mathrm{ev}_B : \frac{\mathbb{F}_q[x]}{(x^d - 1)} \ni \sum_{a=1}^{d} f_a x^a \mapsto \sum_{b=1}^{d} \left(\sum_{a=1}^{d} f_a \beta^{ab} \right) x^b.$$

$$\begin{array}{ccc}
\dfrac{\mathbb{F}_q[x]}{(x^{d+1} - x)} & \xrightarrow{\mathrm{ev}_1} & \dfrac{\mathbb{F}_q[x]}{(x^{d+1} - x)} \\
\Big\downarrow \mathrm{mod}\,(x) \;\Big\downarrow \mathrm{mod}\,(x^d - 1) & & \mathrm{Proj}_A^{A \cup B} \Big\downarrow \mathrm{Proj}_B^{A \cup B} \\
\dfrac{\mathbb{F}_q[x]}{(x)} \bigoplus \dfrac{\mathbb{F}_q[x]}{(x^d - 1)} & \xrightarrow[\mathrm{ev}_A \bigoplus \mathrm{ev}_B]{} & \dfrac{\mathbb{F}_q[x]}{(x)} \bigoplus \dfrac{\mathbb{F}_q[x]}{(x^d - 1)}
\end{array}$$

$$\therefore \ \mathrm{ev}_1^{-1} = \left(\mathrm{mod}\, x \bigoplus \mathrm{mod}\,(x^d - 1) \right)^{-1} \circ \left(\mathrm{ev}_A^{-1} \bigoplus \mathrm{ev}_B^{-1} \right) \circ \left(\mathrm{Proj}_A^{A \cup B} \bigoplus \mathrm{Proj}_B^{A \cup B} \right)$$

$$\mathrm{ev}_A^{-1} : f_0 \mapsto f_0, \quad \mathrm{ev}_B^{-1} : \sum_{a=1}^{d} f_a x^a \mapsto \frac{1}{d} \sum_{b=1}^{d} \left(\sum_{a=1}^{d} f_a \beta^{-ab} \right) x^b$$

Chinese remainder theorem

Because of $\gcd\left(x, x^d - 1\right) = 1$, we have $-\left(x^d - 1\right) + x^{d-1}x = 1$.

Then $\left(\mathrm{mod}\,(x) \bigoplus \mathrm{mod}\,(x^d - 1)\right)^{-1}$ is given by

$$\frac{\mathbb{F}_q[x]}{(x)} \bigoplus \frac{\mathbb{F}_q[x]}{(x^d - 1)} \ni (f, g) \mapsto \boxed{-(x^d - 1)f + x^d g} \in \frac{\mathbb{F}_q[x]}{(x^{d+1} - x)}$$

$$\because\ -(x^d - 1)f + x^d g \equiv f \bmod (x), \quad -(x^d - 1)f + x^d g \equiv g \bmod (x^d - 1).$$

Let $f := f_0$, $g := \dfrac{1}{d}\displaystyle\sum_{b=1}^{d}\left(\sum_{a=1}^{d} f_a \beta^{-ab}\right)x^b$.

Because of $x^d x^b \equiv x^b \bmod \left(x^{d+1} - x\right)$ for $b = 1, \cdots, d$,

$$\mathrm{ev}_1^{-1}(f) = f_0\left(1 - x^d\right) + \frac{1}{d}\sum_{b=1}^{d}\left\{f\left(\beta^{-b}\right) - f(0)\right\}x^b$$

Inverse transform ev_n^{-1}

Example (Formula for ev_1^{-1})

Let $q = 7$, $d = 3$, and $\beta = 2$. For $f = \sum_{a=0}^{3} f_a x^a \in \dfrac{\mathbb{F}_q[x]}{(x^4 - x)}$,

$$\mathrm{ev}_1(f) = \sum_{a=0}^{3} g_a x^a, \quad (g_0, g_1, g_2, g_3) = (f_0, f_1, f_2, f_3) \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 2 & 4 & 1 \\ 0 & 4 & 2 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

$$\mathrm{ev}_1^{-1}(f) = f_0 \left(1 - x^d\right) + \tfrac{1}{d} \sum_{b=1}^{d} \left\{ f\left(\beta^{-b}\right) - f(0) \right\} x^b$$

$$\mathrm{ev}_1^{-1}(g) = \sum_{a=0}^{3} f_a x^a, \quad (f_0, f_1, f_2, f_3) = (g_0, g_1, g_2, g_3) \begin{pmatrix} 1 & 0 & 0 & 6 \\ 0 & 6 & 3 & 5 \\ 0 & 3 & 6 & 5 \\ 0 & 5 & 5 & 5 \end{pmatrix}$$

$$3 \begin{pmatrix} 6 & 3 & 5 \\ 3 & 6 & 5 \\ 5 & 5 & 5 \end{pmatrix} = \begin{pmatrix} 4 & 2 & 1 \\ 2 & 4 & 1 \\ 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} \beta^{-1} & \beta^{-2} & \beta^{-3} \\ \beta^{-2} & \beta^{-4} & \beta^{-6} \\ \beta^{-3} & \beta^{-6} & \beta^{-9} \end{pmatrix}$$

Contents

Comparison of computational complexity

Thus, $F_* = \mathrm{ev}_n^{-1} \circ F_\odot \circ (\mathrm{ev}_n \times \mathrm{ev}_n)$, i.e.,

$$\begin{array}{ccc} R_n \times R_n & \xrightarrow{\mathrm{ev}_n \times \mathrm{ev}_n} & R_n \times R_n \\ {\scriptstyle F_*}\downarrow & & \downarrow{\scriptstyle F_\odot} \\ R_n & \xleftarrow[\mathrm{ev}_n^{-1}]{} & R_n. \end{array}$$

Table: The computational complexity of two multiplication methods.

Multiplication method	F_*	$\mathrm{ev}_n^{-1} \circ F_\odot \circ (\mathrm{ev}_n \times \mathrm{ev}_n)$
Complexity	$\mathrm{O}\left(\prod_{i=1}^{n}(d_i+1)^2\right)$	$\mathrm{O}\left(\left(\sum_{i=1}^{n}(d_i+1)\right)\prod_{i=1}^{n}(d_i+1)\right)$

Contents

[3] Transposed map of ev_n

Let $g \mid (x^q - x)$ and $D = \{\omega \in \mathbb{F}_q \mid g(\omega) = 0\}$.

$$\begin{array}{ccc} \dfrac{\mathbb{F}_q[x]}{(x^q - x)} & \xrightarrow{\mathrm{ev}_1} & \dfrac{\mathbb{F}_q[x]}{(x^q - x)} \\ {\scriptstyle \mathrm{mod}(g)}\downarrow & & \downarrow{\scriptstyle \mathrm{Proj.}} \\ \dfrac{\mathbb{F}_q[x]}{(g)} & \xrightarrow[\mathrm{ev}_D]{} & \dfrac{\mathbb{F}_q[x]}{(g)} \end{array} \Rightarrow \text{transpose} \Rightarrow \begin{array}{ccc} \dfrac{\mathbb{F}_q[x]}{(x^q - x)} & \xleftarrow{\mathrm{ev}_1^\top} & \dfrac{\mathbb{F}_q[x]}{(x^q - x)} \\ \mathcal{E}\uparrow & & \uparrow{\scriptstyle \mathrm{Inc.}} \\ \dfrac{\mathbb{F}_q[x]}{(g)} & \xleftarrow[\mathrm{ev}_D^\top]{} & \dfrac{\mathbb{F}_q[x]}{(g)}, \end{array}$$

where $\mathcal{E}$ denotes "extension" map by linear recurrence relation from g.

ev_1 and $\left(\mathrm{ev}_1^\top\right)^{-1}$ encodes dual error-correcting codes by g, respectively.
$\left(\mathrm{ev}_1^\top\right)^{-1} \circ \mathcal{E}$ is used in systematic encoding.

---

[3] H. Matsui, "Lemma for linear feedback shift registers and DFTs applied to affine variety codes," IEEE Transactions on Information Theory, vol.60, no.5, pp.2751–2769, May 2014.

Example ($n = 1$, $q = 7$, $d_1 = 6$, $\beta_1 = 3$)

For $f = \sum_{a=0}^{6} f_a x^a \in \dfrac{\mathbb{F}_q[x]}{(x^7 - x)}$, $\mathrm{ev}_1(f) = \sum_{a=0}^{6} g_a x^a$, where

$$(g_0, \cdots, g_6) = (f_0, \cdots, f_6) \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 3 & 2 & 6 & 4 & 5 & 1 \\ 0 & 2 & 4 & 1 & 2 & 4 & 1 \\ 0 & 6 & 1 & 6 & 1 & 6 & 1 \\ 0 & 4 & 2 & 1 & 4 & 2 & 1 \\ 0 & 5 & 4 & 6 & 2 & 3 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}, \quad \mathrm{ev}_1^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 6 \\ 0 & 2 & 3 & 1 & 5 & 4 & 6 \\ 0 & 3 & 5 & 6 & 3 & 5 & 6 \\ 0 & 1 & 6 & 1 & 6 & 1 & 6 \\ 0 & 5 & 3 & 6 & 5 & 3 & 6 \\ 0 & 4 & 5 & 1 & 3 & 2 & 6 \\ 0 & 6 & 6 & 6 & 6 & 6 & 6 \end{pmatrix}.$$

$\left(\mathrm{ev}_1^{\top}\right)^{-1}(0, 0, 0, 0, 2, 4, 3) = (4, 2, 2, 6, 5, 4, 5)$ and
$\mathrm{ev}_1(5, 3, 6, 1, 0, 0, 0) = (5, 4, 1, 0, 2, 1, 1)$ are orthogonal.

Let $D = \{3, 3^2, 3^3, 3^4\}$, then $g = 4 + 2x + 3x^2 + 6x^3 + x^4$,
$\mathrm{ev}_1^{\top}(4, 0, 0, 0, 0, 4, 5) = (6, 4, 0, 1, 6, 3, 2)$,
$\mathcal{E}(6, 4, 0, 1) = (6, 4, 0, 1, 4, 6, 6)$, e.g., $-(4, 2, 3, 6) * (6, 4, 0, 1)^T = 4$.
$\left(\mathrm{ev}_1^{\top}\right)^{-1}(6, 4, 0, 1, 4, 6, 6) = (0, 5, 5, 1, 2, 0, 0)$.
$(5, 5, 1, 2)$ agrees with the minus of the redundant part $(2, 2, 6, 5)$.

Tensor-product structure

Example ($n = 2$, $q = 7$, $(d_1, d_2) = (2, 3)$, $(\beta_1, \beta_2) = (6, 2)$)

$$\mathrm{ev}_2(f) = g,\ (f_{(0,0)}, f_{(1,0)}, f_{(2,0)}, \cdots, f_{(2,3)})\, M = (g_{(0,0)}, g_{(1,0)}, g_{(2,0)}, \cdots, g_{(2,3)}),$$

$$M = \begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 6 & 1 & 0 & 6 & 1 & 0 & 6 & 1 & 0 & 6 & 1 \\
0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\
0 & 0 & 0 & 2 & 2 & 2 & 4 & 4 & 4 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 5 & 2 & 0 & 3 & 4 & 0 & 6 & 1 \\
0 & 0 & 0 & 0 & 2 & 2 & 0 & 4 & 4 & 0 & 1 & 1 \\
0 & 0 & 0 & 4 & 4 & 4 & 2 & 2 & 2 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 3 & 4 & 0 & 5 & 2 & 0 & 6 & 1 \\
0 & 0 & 0 & 0 & 4 & 4 & 0 & 2 & 2 & 0 & 1 & 1 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 6 & 1 & 0 & 6 & 1 & 0 & 6 & 1 \\
0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1
\end{pmatrix},$$

which is the Kronecker-product matrix $\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 2 & 4 & 1 \\ 0 & 4 & 2 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 1 & 1 \\ 0 & 6 & 1 \\ 0 & 1 & 1 \end{pmatrix}$.

Conclusion and future works

Efficient one-to-one and onto between multiple-valued logic functions

$$F : \Omega_n = \left\{\omega_1 \in \mathbb{F}_q \,\middle|\, \omega_1^{d_1+1} = \omega_1\right\} \times \cdots \times \left\{\omega_n \in \mathbb{F}_q \,\middle|\, \omega_n^{d_n+1} = \omega_n\right\} \to \mathbb{F}_q,$$

where $d_i \mid (q-1)$, and multiple-valued logic polynomials

$$f = f(x_1, \cdots, x_n) = \sum_{a_1=0}^{d_1} \cdots \sum_{a_n=0}^{d_n} f_{(a_1,\cdots,a_n)} x_1^{a_1} \cdots x_n^{a_n}, \quad f_{(a_1,\cdots,a_n)} \in \mathbb{F}_q,$$

i.e., $\mathrm{ev}_n(f) = F$ and $\mathrm{ev}_n^{-1}(F) = f$ with $\mathrm{O}\left(\left(\sum_{i=1}^{n}(d_i+1)\right)\prod_{i=1}^{n}(d_i+1)\right)$.

Future works
- $D_1 \times D_2$, $D_1 \cap D_2$, $D_1 \cup D_2$, $D_1 - D_2$ for $D_1, D_2 \subset \left(\mathbb{F}_q\right)^n$
- Connection with ZDD and practical applications