On Formal Expressions of BRW-polynomials

Guillermo Morales-Luna
Computer Science Department
CINVESTAV-IPN
gmorales@cs.cinvestav.mx

January 3, 2013

Abstract

Algebraic expressions of the Bernstein-Rabin-Winograd-polynomials, when defined over the field of the rational numbers, are obtained by recursion.

1 Introduction

For the purpose of message authentication, a family of polynomial hash functions was introduced in [1], the so called *Bernstein-Rabin-Winograd* (BRW) polynomials. The *tweakable enciphering schemes* [3], mostly applied on low-level disk encryption systems make, an extensive use of the BRW-polynomials due to the implicit economy in their computations. Efficient pipelined algorithms, with ad-hoc hardware implementation, were developed in [2], achieving great performances. For most applications the BRW-polynomials are considered on polynomial rings over finite fields.

A family of BRW-polynomials is a sequence defined recursively and its construction rules make the sequence quite suitable for efficient evaluation. For a fixed sequence of parameters, an index and a field element, the value of the corresponding polynomial on that element is efficiently computed, those for authentication and signing purposes they provide an important family of hashing maps.

In this short note we study the BRW-polynomials over the field of rational numbers and the resulting recursive relations in order to fully express in their algebraic forms the BRW-polynomials. An elementary remark [1], is the assertion that the BRW-polynomials have degrees one less than a power of two. For a fixed set of parameters determining the coefficients of the BRW-polynomials, the set of indexes can be partitioned by cuts at the powers of two, and within such a block several common characteristic features of the BRW-polynomials are distinguished allowing to calculate completely the algebraic forms in linear time complexity with respect to the block index, although in exponential space complexity.

2 BRW-polynomials

Let us consider the polynomial ring $\mathbb{Q}[X]$ over the field $\mathbb{Q}$ of rational numbers. For a given rational sequence $\mathbf{c} = (c_i)_{i\in\mathbb{N}}$, let us denote by $\mathbf{c}_j$, for each $j \in \mathbb{N}$, the sequence obtained by dropping the first j terms at $\mathbf{c}$: $\mathbf{c}_j = (c_i)_{i\geq j}$. Hence, $\mathbf{c}_0 = \mathbf{c}$.

Given $\mathbf{c} = (c_i)_{i\in\mathbb{N}}$, the corresponding sequence of *Bernstein-Rabin-Winograd* (BRW) polynomials $H = (H_{m,\mathbf{c}})_{m\in\mathbb{N}}$ is defined inductively as follows:

$$\begin{aligned}
H_{0,\mathbf{c}}(X) &= 0\\
H_{1,\mathbf{c}}(X) &= c_0\\
H_{2,\mathbf{c}}(X) &= c_0 + c_1X\\
H_{3,\mathbf{c}}(X) &= (c_0 + X)\cdot(c_1 + X^2) + c_2 \qquad (1)\\
\forall k > 3: \quad H_{m,\mathbf{c}}(X) &= H_{m_0-1,\mathbf{c}}(X)\cdot(c_{m_0-1} + X^{m_0}) + H_{m-m_0,\mathbf{c}_{m_0}}(X),\ \text{where } m_0 = 2^{\lfloor\log_2 m\rfloor}. \qquad (2)
\end{aligned}$$

Remark 2.1 *For each $m \geq 4$, the polynomial $H_{m,\mathbf{c}}(X) \in \mathbb{Q}[X]$ has degree $2^{1+\lfloor \log_2 m \rfloor} - 1$.*

Namely, reasoning by induction, we see that for $m = 4$, from (2), $H_{4,\mathbf{c}}(X) = H_{3,\mathbf{c}}(X) \cdot (c_3 + X^4) + H_{0,\mathbf{c}_4}(X)$ and it has degree $7 = 2^3 - 1$. For $m > 4$ let us write $m = 2^{m_0} + m_1$, where $m_0 = 2^{\lfloor \log_2 m \rfloor}$. From (2) it follows that the degree of $H_{m,\mathbf{c}}(X)$ is

$$\deg H_{m_0,\mathbf{c}}(X) + m_0 = 2^{1+\lfloor \log_2 (m_0 - 1) \rfloor} - 1 + 2^{\lfloor \log_2 m \rfloor} = 2 \cdot 2^{\lfloor \log_2 m \rfloor} - 1.$$

For any $n \in \mathbb{Z}^+$ let $I_n = \{2^{n-1}, \ldots, 2^n - 1\}$: $I_1 = \{1\}$, $I_2 = \{2, 3\}$, $I_3 = \{4, 5, 6, 7\}$, $I_4 = \{8, \ldots, 15\}$, ... Thus $(I_n)_{n \in \mathbb{Z}^+}$ is a partition of $\mathbb{Z}^+$ consisting of sets of consecutive integers delimited by powers of 2. The remark 2.1 can be restated as:

Remark 2.2 *For each $n \geq 3$: $[m \in I_n \implies \deg H_{m,\mathbf{c}}(X) = 2^n - 1]$.*

Hence, for $m \in I_n$ the coefficient vector of the polynomial $H_{m,\mathbf{c}}(X)$ has dimension 2^n, thus the polynomial expression can be split into two parts, a *lower part* and an *upper part*, each determined by 2^{n-1} coefficients. Let us write:

$$H_{m,\mathbf{c}}(X) = G^{\ell}_{m,\mathbf{c}}(X) + G^{u}_{m,\mathbf{c}}(X) \cdot X^{2^{n-1}}. \tag{3}$$

Let us compare (3) with (2).

Since $m \in I_n$, $\lfloor \log_2 m \rfloor = n - 1$ and $m_0 = 2^{n-1}$,

$$\begin{aligned} G^{\ell}_{m,\mathbf{c}}(X) + G^{u}_{m,\mathbf{c}}(X) \cdot X^{2^{n-1}} &= H_{2^{n-1}-1,\mathbf{c}}(X) \cdot (c_{2^{n-1}-1} + X^{2^{n-1}}) + H_{m-2^{n-1},\mathbf{c}_{2^{n-1}}}(X) \\ &= \left(H_{m-2^{n-1},\mathbf{c}_{2^{n-1}}}(X) + c_{2^{n-1}-1} \, H_{2^{n-1}-1,\mathbf{c}}(X) \right) + H_{2^{n-1}-1,\mathbf{c}}(X) \cdot X^{2^{n-1}}. \end{aligned}$$

But $m - 2^{n-1} < 2^{n-1}$, thus by remark 2.2, $\deg H_{2^{n-1}-1,\mathbf{c}}(X), \deg H_{2^{n-1}-1,\mathbf{c}}(X) < 2^{n-1}$, hence

$$\begin{aligned} G^{\ell}_{m,\mathbf{c}}(X) &= H_{m-2^{n-1},\mathbf{c}_{2^{n-1}}}(X) + c_{2^{n-1}-1} \, H_{2^{n-1}-1,\mathbf{c}}(X) && (4) \\ G^{u}_{m,\mathbf{c}}(X) &= H_{2^{n-1}-1,\mathbf{c}}(X). && (5) \end{aligned}$$

The relation (5) means that the upper part is the same polynomial for all $m \in I_n$.

For each $k \geq 2$, let

$$F^{\ell}_{k,\mathbf{c}}(X) = G^{\ell}_{2^k,\mathbf{c}}(X) \quad \text{and} \quad F^{u}_{k,\mathbf{c}}(X) = G^{u}_{2^k,\mathbf{c}}(X). \tag{6}$$

Again, $F^{u}_{k,\mathbf{c}}(X)$ is a polynomial of degree $2^k - 1$ and it is determined by a coefficient vector of dimension 2^k, hence it can be split into a lower and an upper parts. Let us express it as

$$F^{u}_{k,\mathbf{c}}(X) = F^{u\ell}_{k,\mathbf{c}}(X) + F^{uu}_{k,\mathbf{c}}(X) \cdot X^{2^{k-1}}. \tag{7}$$

Now, let us observe that

$$\begin{aligned} F^{u}_{k,\mathbf{c}}(X) &= G^{u}_{2^k,\mathbf{c}}(X) \\ &= H_{2^k-1,\mathbf{c}}(X) \\ &= H_{2^{k-1}-1,\mathbf{c}}(X) \cdot (c_{2^{k-1}-1} + X^{2^{k-1}}) + H_{2^k-1-2^{k-1},\mathbf{c}_{2^{k-1}}}(X) \\ &= \left(H_{2^{k-1}-1,\mathbf{c}_{2^{k-1}}}(X) + c_{2^{k-1}-1} \cdot H_{2^{k-1}-1,\mathbf{c}}(X) \right) + H_{2^{k-1}-1,\mathbf{c}}(X) \cdot X^{2^{k-1}}, \end{aligned}$$

since $\deg H_{2^{k-1}-1,\mathbf{c}_{2^{k-1}}}(X) = \deg H_{2^{k-1}-1,\mathbf{c}}(X) = 2^{k-2}$, we obtain, from (7):

$$\begin{aligned} F^{u\ell}_{k,\mathbf{c}}(X) &= H_{2^{k-1}-1,\mathbf{c}_{2^{k-1}}}(X) + c_{2^{k-1}-1} \cdot H_{2^{k-1}-1,\mathbf{c}}(X) \\ F^{uu}_{k,\mathbf{c}}(X) &= H_{2^{k-1}-1,\mathbf{c}}(X), \end{aligned}$$

and these equations, together with (5) and (6), can be restated as:

$$\begin{aligned} F^{u\ell}_{k,\mathbf{c}}(X) &= F^{u}_{k-1,\mathbf{c}_{2^{k-1}}}(X) + c_{2^{k-1}-1} \cdot F^{u}_{k-1,\mathbf{c}}(X) && (8) \\ F^{uu}_{k,\mathbf{c}}(X) &= F^{u}_{k-1,\mathbf{c}}(X). && (9) \end{aligned}$$

Clearly, the relations (7), (8) and (9) pose the following recurrence relation for the polynomial sequence $F^u_{\mathbf{c}} = \left(F^u_{k,\mathbf{c}}(X)\right)_{k\geq 2}$:

$$\forall k > 2: \quad F^u_{k,\mathbf{c}}(X) = \left(F^u_{k-1,\mathbf{c}_{2^{k-1}}}(X) + c_{2^{k-1}-1} \cdot F^u_{k-1,\mathbf{c}}(X)\right) + F^u_{k-1,\mathbf{c}}(X) \cdot X^{2^{k-1}}. \tag{10}$$

For the base case of this recurrence, we observe that, from (1): $H_{3,\mathbf{c}}(X) = (c_0c_1 + c_2) + c_1X + (c_0 + X)\,X^2$, thus we may define

$$F^u_{1,\mathbf{c}}(X) = c_0 + X,$$

and (10) holds $\forall k \geq 2$.

The relations (4), (5) can be rewritten, using (9), as

$$\begin{aligned} G^u_{m,\mathbf{c}}(X) &= F^u_{n-1,\mathbf{c}}(X) \\ G^\ell_{m,\mathbf{c}}(X) &= H_{m-2^{n-1},\mathbf{c}_{2^{n-1}}}(X) + c_{2^{n-1}-1}\, F^u_{n-1,\mathbf{c}}(X) \end{aligned} \tag{11}$$

and finally, from (5)

$$\forall m \in I_n: \quad H_{m,\mathbf{c}}(X) = \left(H_{m-2^{n-1},\mathbf{c}_{2^{n-1}}}(X) + c_{2^{n-1}-1}\, F^u_{n-1,\mathbf{c}}(X)\right) + F^u_{n-1,\mathbf{c}}(X) \cdot X^{2^{n-1}}. \tag{12}$$

Equation (12) gives a recursive procedure to calculate the formal polynomial expression of the BRW-polynomial $H_{m,\mathbf{c}}(X)$.

Some direct conclusions follow:

- With respect to analysis, the BRW-polynomials differ slightly for indexes within I_n:

$$\forall m \in I_n: \; H_{m,\mathbf{c}}(X) = F^u_{n-1,\mathbf{c}}(X) \cdot X^{2^{n-1}} + o(X^{2^{n-1}}).$$

- The algorithm determined by (12) has time complexity $O(n)$ although it has space complexity $O(2^n)$.
- The right hand side of (8) is the addition of a polynomial, let us say $\sum_{j=0}^{2^{k-1}-1} a_j X^j$, and a constant multiple of other polynomial of the same degree, let us say $\sum_{j=0}^{2^{k-1}-1} b_j X^j$. Thus, the left hand side can be calculated as $\sum_{j=0}^{2^{k-1}-1} A(a_j, c_{2^{k-1}-1}, b_j)X^j$, where $A : (a, c, b) \mapsto a + c \cdot b$.
- The first summand at the right hand side of (12), which is given by (11), can be calculated as well through the map A at the point before.
- The coefficients of the BRW-polynomials are calculated by iterations of the operator A acting over the coefficient list $\mathbf{c}$, and the involved computations can be parallelized.

References

[1] Daniel J. Bernstein. Polynomial evaluation and message authentication, 2007. `http://cr.yp.to/papers.html#pema`.

[2] Debrup Chakraborty, Cuauhtemoc Mancillas-Lopez, Francisco Rodriguez-Henriquez, and Palash Sarkar. Efficient hardware implementations of BRW polynomials and tweakable enciphering schemes. *IEEE Transactions on Computers*, 62(2):279–294, 2013.

[3] Palash Sarkar. Efficient tweakable enciphering schemes from (block-wise) universal hash functions. *IEEE Trans. Inf. Theor.*, 55(10):4749–4760, October 2009.