# A New Representation of Elements of Binary Fields with Subquadratic Space Complexity Multiplication

Sedat Akleylek Murat Cenk Ferruh Özbudak

Institute of Applied Mathematics,
Middle East Technical University,
Ankara, TURKEY
*http://www.iam.metu.edu.tr*

# Outline

## Polynomial Representation

- $GF(2^n)$ can be viewed as a vector space of dimension $n$ over $GF(2)$. Then, any basis of $GF(2^n)$ over $GF(2)$ can be used to represent the elements in $GF(2^n)$.
- A monic polynomial $a(x)$ over $GF(2)$ of degree $n$ is of the form

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

  with $a_i \in GF(2)$ for $0 \leq i < n$.
- $GF(2^n)$ is constructed by taking the quotient of $GF(2)[x]$ with an irreducible polynomial $f$ of degree $n$ i.e. $GF(2^n) \cong GF(2)[x]/(f)$.

- The finite field is represented as polynomials of degree less than $n$ with coefficients in $GF(2)$.
- Addition is performed term-wise.
- The binary extension field multiplication can be performed in two steps: multiplication over $GF(2)$ and modular reduction over $GF(2^n)$.
- The complexity of finite field multiplication depends on the number of non-zero terms in the irreducible reduction polynomials. Therefore, it is desirable to use the reduction polynomials with as few non-zero terms as possible for efficient implementations.

# Irreducible Polynomials

- These correspond trinomials ($x^n + x^k + 1$, for $k > 0$) and pentanomials ($x^n + x^{k_1} + x^{k_2} + x^{k_3} + 1$, for $0 < k_3 < k_2 < k_1$) over $GF(2)$.
- Trinomials over $GF(2)$ do not exist for all degree $n$.
- When an irreducible trinomial of degree $n$ does not exist, it is recommended to use an irreducible pentanomial. There is no known value of $n$ for which an irreducible polynomial of weight $w \leq 5$ does not exist.

## Motivation

- Our aim is to obtain binomial, trinomial or quadranomial irreducible polynomials in any representation which allows us multiplication with subquadratic space complexity and faster modular reduction over binary fields when there is no desirable such low weight irreducible polynomial in other representations.

## Previous Work

- Hasan and Negre study Dickson polynomials for binary field representation (WAIFI 2008).
- Dickson polynomials seem interesting when no optimal normal basis (ONB) in any type exists for the field. This is the case for NIST recommended binary fields $GF(2^{163})$ and $GF(2^{283})$.
- They formulate finite field multiplication as a product of a Toeplitz or Hankel matrix and a vector with subquadratic space complexity multipliers.

## Definition

The Hermite polynomials are $H_0(x) = 1$, $H_1(x) = x$ with the recursion

$$H_n(x) = x \cdot H_{n-1}(x) - (n-1) \cdot H_{n-2}(x)$$

for $n \geq 2$.

We obtain the Hermite polynomials in $GF(2)[x]$ for $n \leq 10$.

$H_0(x) = 1$, $H_1(x) = x$, $H_2(x) = x^2 + 1$,
$H_3(x) = x^3 + x$,
$H_4(x) = x^4 + 1$,
$H_5(x) = x^5 + x$,
$H_6(x) = x^6 + x^4 + x^2 + 1$,
$H_7(x) = x^7 + x^5 + x^3 + x$,
$H_8(x) = x^8 + 1$,
$H_9(x) = x^9 + x$,
$H_{10}(x) = x^{10} + x^8 + x^2 + 1$.

# Multiplication in Hermite Polynomials

## Theorem

*Let $H_n(x) = \beta_n$ be the $n$-th Hermite polynomial in $GF(2)[x]$, where $n \geq 0$. Then, for all $i, j \geq 0$ Hermite basis satisfies the following equation*

$$\beta_i \cdot \beta_j = \beta_{i+j} + \ell \cdot \beta_{i+j-2}$$

*where $\ell \in GF(2)$. If $i$ and $j$ are both odd number, then $\ell = 1$. If $i$ or $j$ is an even number, then $\ell = 0$.*

Theorem can be proved by using induction on $i$ and $j$. Note that we are working on binary fields.

# Hermite Polynomials

**Theorem**

*Let $f$ be an irreducible polynomial of degree $n$ in $GF(2)[x]$. The set $\{\beta_0, \beta_1, \cdots, \beta_{n-1}\}$ forms a basis of $GF(2^n) \cong GF(2)[x]/(f)$.*

**Proof.**

Sketch of the proof

- Each element in $GF(2^n)$ is expressed by using the set $\{\beta_0, \beta_1, \cdots, \beta_{n-1}\}$.
- Then, we need to show that this representation is unique.

- Let $a(x) = a'_{n-1}x^{n-1} + \cdots + a'_1 x + a'_0$, where $a'_i \in GF(2)$ be a polynomial with the standard representation. $a(x)$ can be represented by using Hermite polynomials as $a = a_{n-1}\beta_{n-1} + \cdots + a_1\beta_1 + a_0\beta_0$, where $a_i \in GF(2)$.

**Algorithm 1** Conversion of Coefficients From Polynomial Representation to Hermite Polynomial Representation

**Input:** $a(x) = \sum_{i=0}^{n-1} a'_i x^i$
**Output:** $(a_0, a_1, \cdots, a_{n-1})$, where $a = \sum_{i=0}^{n-1} a_i \beta_i$

```
1: T ← a
2: for i = n downto 1 do
3:     if deg(T) = i then
4:         a_i ← 1
5:         T ← T + β_i
6:     else
7:         a_i ← 0
8:     end if
9: end for
10: a_0 ← T
```

# Polynomial Multiplication Using Hermite Polynomials Over Binary Fields

## Example

Let $a = a_3\beta_3 + a_2\beta_2 + a_1\beta_1 + a_0\beta_0$ and
$b = b_3\beta_3 + b_2\beta_2 + b_1\beta_1 + b_0\beta_0$ be 4-term polynomials over $GF(2)$.
Let $a \cdot b = c = c_6\beta_6 + \cdots + c_0\beta_0$. Then,

$$
\begin{aligned}
c_0 &= a_0b_0 + \underline{a_1b_1} \\
c_1 &= a_0b_1 + a_1b_0 \\
c_2 &= a_0b_2 + a_2b_0 + a_1b_1 + \underline{a_1b_3} + \underline{a_3b_1} \\
c_3 &= a_0b_3 + a_3b_0 + a_1b_2 + a_2b_1 \\
c_4 &= a_1b_3 + a_3b_1 + a_2b_2 + \underline{a_3b_3} \\
c_5 &= a_2b_3 + a_3b_2 \\
c_6 &= a_3b_3
\end{aligned}
$$

## Continued

### Example

$a_1b_1$, $(a_1b_3 + a_3b_1)$ and $a_3b_3$ are the extra terms when we compare this multiplication with polynomial basis representation. The computation of these extra terms can be achieved by the following method:
Let $x_0 = a_1$, $y_0 = b_1$, $x_1 = a_3$ and $y_1 = b_3$. Then, the extra terms can be written as follows:
$m_1 = x_0y_0$, $m_2 = (x_0 + x_1)(y_0 + y_1) - m_1 - m_3$ and $m_3 = x_1y_1$.
The computation of $a \cdot b = c = c_6\beta_6 + \cdots + c_0\beta_0$ is $9 + 3 = 12$ multiplications and $24 + 4 + 3 = 31$ additions by using Karatsuba method.

# Polynomial Multiplication Using Hermite Polynomials Over Binary Fields

## Theorem

*Let $n = p^j$, where $p$ is a prime number and $j$ is a positive integer. Let $a = a_{n-1}\beta_{n-1} + \cdots + a_0\beta_0$ and $b = b_{n-1}\beta_{n-1} + \cdots + b_0\beta_0$ be $n$-term polynomials over $GF(2)$ and $a \cdot b = c = c_{2n-2}\beta_{2n-2} + \cdots + c_0\beta_0$. Then,*

1. *If $p = 2$, the required number of multiplications is $n^{log_2 3} + \left\lfloor \frac{n}{2} \right\rfloor^{log_2 3}$ and the required number of additions is $8n^{log_2 3} - 11n + 3$.*
2. *If $p = 3$, the required number of multiplications is $n^{log_3 6} + \left\lfloor \frac{n}{2} \right\rfloor^{log_3 6}$ and the required number of additions is $\frac{116}{15}n^{log_3 6} - \frac{29}{5}n + \frac{7}{5}$.*

*by using Karatsuba multiplication method.*

# Irreducible Hermite Binomials

$$
\begin{array}{cc}
f = \beta_3 + \beta_0 & f = \beta_2 + \beta_1 \\
f = \beta_7 + \beta_0 & f = \beta_4 + \beta_1 \\
f = \beta_9 + \beta_0 & f = \beta_6 + \beta_1 \\
f = \beta_{15} + \beta_0 & f = \beta_{22} + \beta_1 \\
f = \beta_{63} + \beta_0 & f = \beta_{28} + \beta_1 \\
f = \beta_{127} + \beta_0 & f = \beta_{46} + \beta_1 \\
f = \beta_{471} + \beta_0 & f = \beta_{52} + \beta_1
\end{array}
$$

# Reduction of Polynomials Using Irreducible Hermite Binomials

Let $f = \beta_n + \beta_0$ be an irreducible polynomial of degree $n$ over $GF(2)$. Let $n \leq i \leq 2n-2$. Then,

$$\begin{aligned} \beta_n \beta_{i-n} &= \beta_i + \beta_{i-2} \cdot \ell \\ \beta_0 \beta_{i-n} &= \beta_i + \beta_{i-2} \cdot \ell \\ \beta_i &= \beta_{i-n} + \beta_{i-2} \cdot \ell \end{aligned}$$

If $i-n$ is odd, then $\ell = 1$. Otherwise, $\ell = 0$.

# Reduction of Polynomials Using Irreducible Hermite Binomials

Let $f = \beta_n + \beta_1$ be an irreducible polynomial of degree $n$ over $GF(2)$. Let $n \leq i \leq 2n-2$. Then,

$$\begin{aligned} \beta_n \beta_{i-n} &= \beta_i + \beta_{i-2} \cdot \ell \\ \beta_1 \beta_{i-n} &= \beta_i + \beta_{i-2} \cdot \ell \\ \beta_i &= \beta_{i-n+1} + (\beta_{i-2} + \beta_{i-n-1}) \cdot \ell \end{aligned}$$

If $i-n$ is odd, then $\ell = 1$. Otherwise, $\ell = 0$.

# Irreducible Hermite Trinomials

$$
\begin{array}{ll}
f = \beta_{137} + \beta_{17} + \beta_0 & f = \beta_{113} + \beta_{12} + \beta_1 \\
f = \beta_{169} + \beta_5 + \beta_0 & f = \beta_{199} + \beta_{28} + \beta_1 \\
f = \beta_{223} + \beta_{17} + \beta_0 & f = \beta_{271} + \beta_{24} + \beta_1 \\
\underline{f = \beta_{233} + \beta_5 + \beta_0} & f = \beta_{209} + \beta_{26} + \beta_1 \\
f = \beta_{271} + \beta_7 + \beta_0 & f = \beta_{281} + \beta_6 + \beta_1 \\
f = \beta_{311} + \beta_{25} + \beta_0 & \underline{f = \beta_{283} + \beta_{66} + \beta_1} \\
f = \beta_{383} + \beta_{21} + \beta_0 & f = \beta_{361} + \beta_{16} + \beta_1 \\
f = \beta_{431} + \beta_{65} + \beta_0 & f = \beta_{457} + \beta_{24} + \beta_1 \\
f = \beta_{497} + \beta_3 + \beta_0 & f = \beta_{491} + \beta_{26} + \beta_1 \\
f = \beta_{577} + \beta_7 + \beta_0 & \underline{f = \beta_{571} + \beta_{22} + \beta_1} \\
f = \beta_{641} + \beta_{11} + \beta_0 & f = \beta_{653} + \beta_2 + \beta_1
\end{array}
$$

## Reduction of Polynomials Using Irreducible Hermite Trinomials

- Let $f = \beta_n + \beta_k + \beta_0$ be an irreducible polynomial of degree $n$ over $GF(2)$. Let $n \leq i \leq 2n-2$. Then,

$$\beta_i \quad = \quad \beta_{i-n+k} + \beta_{i-n} + \beta_{i-2} \cdot \ell$$

If $i-n$ is odd, then $\ell = 1$. Otherwise, $\ell = 0$.

- Let $f = \beta_n + \beta_k + \beta_1$ be an irreducible polynomial of degree $n$ over $GF(2)$. Let $n \leq i \leq 2n-2$. Then,

$$\beta_i \quad = \quad \beta_{i-n+k} + \beta_{i-n+1} + (\beta_{i-n-1} + \beta_{i-2}) \cdot \ell$$

If $i-n$ is odd, then $\ell = 1$. Otherwise, $\ell = 0$.

# Irreducible Hermite Quadranomials

$$\underline{f = \beta_8 + \beta_4 + \beta_3 + \beta_0} \qquad \underline{f = \beta_8 + \beta_6 + \beta_3 + \beta_0}$$

$$f = \beta_{13} + \beta_4 + \beta_2 + \beta_0 \qquad f = \beta_{16} + \beta_6 + \beta_4 + \beta_1$$

$$f = \beta_{116} + \beta_4 + \beta_2 + \beta_1 \qquad f = \beta_{122} + \beta_6 + \beta_2 + \beta_1$$

$$f = \beta_{227} + \beta_5 + \beta_4 + \beta_1 \qquad f = \beta_{269} + \beta_4 + \beta_2 + \beta_0$$

$$f = \beta_{285} + \beta_5 + \beta_2 + \beta_1 \qquad f = \beta_{307} + \beta_5 + \beta_2 + \beta_1$$

$$f = \beta_{311} + \beta_7 + \beta_4 + \beta_1 \qquad f = \beta_{335} + \beta_9 + \beta_5 + \beta_0$$

$$f = \beta_{361} + \beta_{16} + \beta_2 + \beta_0 \qquad f = \beta_{398} + \beta_7 + \beta_2 + \beta_0$$

$$f = \beta_{403} + \beta_{23} + \beta_3 + \beta_0 \qquad f = \beta_{413} + \beta_{10} + \beta_8 + \beta_0$$

$$f = \beta_{452} + \beta_7 + \beta_4 + \beta_0 \qquad f = \beta_{456} + \beta_7 + \beta_3 + \beta_1$$

**Table:** Reduction Complexity

| | Form | $\#XOR$ |
|---|---|---|
| Hermite Binomial | $\beta_n + \beta_0$ | $2n$ |
| Hermite Binomial | $\beta_n + \beta_1$ | $3n$ |
| Hermite Trinomial | $\beta_n + \beta_k + \beta_0$ | $3n$ |
| Hermite Trinomial | $\beta_n + \beta_k + \beta_1$ | $4n$ |

**Table:** Complexity Comparison of Selected Multipliers

| | $p$ | $\#AND$ | $\#XOR$ |
|---|---|---|---|
| Hermite Binomial | 2 | $n^{log_2 3} + \lfloor \frac{n}{2} \rfloor^{log_2 3}$ | $8n^{log_2 3} - 8n + 3$ |
| Hermite Binomial | 3 | $n^{log_3 6} + \lfloor \frac{n}{2} \rfloor^{log_3 6}$ | $\frac{116}{15} n^{log_3 6} - \frac{14}{5} n + \frac{7}{5}$ |
| Hermite Trinomial | 2 | $n^{log_2 3} + \lfloor \frac{n}{2} \rfloor^{log_2 3}$ | $8n^{log_2 3} - 7n + 3$ |
| Hermite Trinomial | 3 | $n^{log_3 6} + \lfloor \frac{n}{2} \rfloor^{log_3 6}$ | $\frac{116}{15} n^{log_3 6} - \frac{9}{5} n + \frac{7}{5}$ |
| Dickson Binomial | 2 | $2n^{log_2 3}$ | $11n^{log_2 3} - 11n$ |
| Dickson Binomial | 3 | $2n^{log_2 3}$ | $\frac{48}{5} n^{log_3 6} - 11n + \frac{3}{5}$ |
| Dickson Trinomial | 2 | $2n^{log_3 6}$ | $11n^{log_2 3} - 4n + 1$ |
| Dickson Trinomial | 3 | $2n^{log_3 6}$ | $\frac{48}{5} n^{log_3 6} - 2n + \frac{1}{5}$ |
| ONB I | 2 | $n^{log_2 3} + n$ | $\frac{11}{2} n^{log_2 3} - 4n - \frac{1}{2}$ |
| ONB I | 3 | $n^{log_3 6} + n$ | $\frac{24}{5} n^{log_3 6} - 3n - \frac{4}{5}$ |
| ONB II | 2 | $2n^{log_2 3}$ | $11n^{log_2 3} - 12n + 1$ |
| ONB II | 3 | $2n^{log_3 6}$ | $\frac{48}{5} n^{log_3 6} - 10n - \frac{2}{5}$ |

## Conclusion

- We give a new way to represent certain finite fields $GF(2^n)$. This representation is based on Hermite polynomials.
- We show that multiplication in Hermite polynomial representation can be performed with subquadratic space complexity.
- One can obtain binomial, trinomial or quadranomial irreducible polynomials in Hermite polynomial representation which allows us faster modular reduction over binary fields when there is no desirable such low weight irreducible polynomial in other representations.
- This representation is very interesting for NIST recommended binary field $GF(2^{571})$ since there is no ONB for the corresponding extension. We also note that recommended NIST binary fields can be constructed with low weight Hermite polynomials.

Thank you for your attention!