Redundant Representation of Finite Fields

Willi Geiselmann and Harald Lukhaub

Institut für Algorithmen und Kognitive Systeme,
Arbeitsgruppen Computeralgebra & Systemsicherheit, Prof. Dr. Th. Beth,
Universität Karlsruhe, Am Fasanengarten 5, 76 128 Karlsruhe, Germany.

Abstract. A redundant representation of finite fields with 2^n elements is presented. It unifies the advantages of polynomial and normal bases by the cost of redundancy. The arithmetic, especially exponentiation, in this representation is perfectly suited for low power computing: multiplication can be built up with reversible gates very efficient and squaring is a cyclic shift.

1 Introduction

Hardware implementations of cryptographic schemes based on the Discrete Logarithm Problem in $\mathbf{F}_{2^n}$, the field with 2^n elements, (see e.g. [1,2]), require efficient exponentiation architectures.

On the one hand, research has been particularly attracted to the choice of the representation of the field. Dual basis multipliers in $\mathbf{F}_{2^n}$ were first suggested by Berlekamp [14] for encoding Reed-Solomon codes. A representation in a polynomial basis is the standard representation, usually the best choice for general-purpose applications. A very promising approach is the use of a normal basis, where squaring is an extremely simple operation [6,8,11,13]. However, normal basis multiplication can become very complex and good normal bases have to be selected carefully [13]. Especially for exponentiation with low weight exponents the advantage of a normal basis is pronounced.

On the other hand, work on low power computing is coming up more and more. One reason is the problem of cooling of the chips with the increasing integration; another problem in cryptology is the resistance of encrption units against differential power analysis [9].

1.1 Classical Multiplication

In this section a brief overview on different representations of finite fields and the resulting circuits is given. More details can be found in [5,8,15].

Polynomial Basis Multiplication The standard representation of an extension field is the polynomial basis:

Definition 1. *For $n \in \mathbf{N}, n \geq 2$ it holds $\mathbf{F}_{2^n} \simeq \mathbf{F}_2[x]/f(x)$ where $f(x) \in \mathbf{F}_2[x]$ is an irreducible polynomial of degree n. Let $\alpha \in \mathbf{F}_{2^n}$ be a zero of $f(x)$, then $\left(1, \alpha, \ldots, \alpha^{n-1}\right)$ is an $\mathbf{F}_2$ (vector space) basis of $\mathbf{F}_{2^n}$, called a* polynomial basis.

K. Kim (Ed.): PKC 2001, LNCS 1992, pp. 339–352, 2001.
© Springer-Verlag Berlin Heidelberg 2001

In this representation multiplication can easily be performed by linear feedback shift registers (LFSRs), where $f(x)$ is used as the feedback polynomial. One of the possible realizations is given in Figure 1.

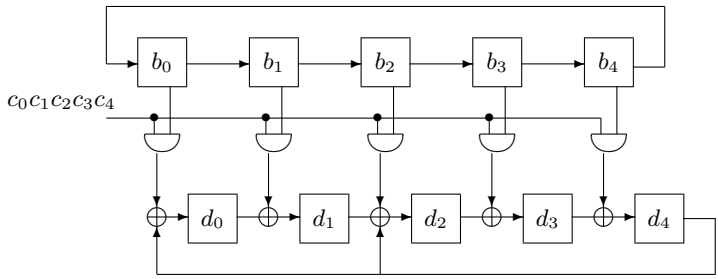


Fig. 1. A polynomial basis multiplier for $\mathbb{F}_{2^5} : \mathbb{F}_2 \bmod f(x) := x^5 + x^2 + 1$.

Normal Basis Multiplication A normal basis of $\mathbb{F}_{2^n}$ is defined as follows.

Definition 2. *A basis* $N = (\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ *of* $\mathbb{F}_{2^n}$ *is called a* normal basis *(over* $\mathbb{F}_2$*) if there exists some* $\alpha \in \mathbb{F}_{2^n}$ *with* $\alpha_i = \alpha^{2^i}$ *for all* i, $0 \leq i < n$.

In a normal basis $(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ of $\mathbb{F}_{2^n}$ squaring is a cyclic shift of coefficients due to

$$\left(\sum_{i=0}^{n-1} u_i \alpha_i\right)^2 = \sum_{i=0}^{n-1} u_i \alpha_{i+1} \quad \text{and } \alpha_n := \alpha^{2^n} = \alpha_0. \tag{1}$$

Multiplication is more difficult as the products $\alpha_i \alpha_j$ are, in general, not elements of the normal basis. The cost of normal basis multiplication is frequently measured by the complexity of the linear combinations needed to represent the elements $\alpha_0 \alpha_i$ in the normal basis [13]. The efficiency of any normal basis multiplier suggested uses field extensions in which good (optimal) normal bases exist [3,13]; in many fields such good normal bases are not available.

1.2 Reversible Computing

From physics it is known that erasure of information (deleting or resetting of storage cells) results in heating up the system. Therefore one approach to design low power computing devices is to use reversible gates [4,12,10]. These gates keep all information, i. e. they are bijections.

Permutations and shifts obviously fulfill this condition.

One basic gate is the Fredkin gate: the inputs `(a, b, c)` are mapped to the outputs `(a, b, c)` if `a = 0`; if the input `a = 1` the outputs `b, c` are exchanged, i. e. the output is `(a, c, b)`.

Another reversible gate is the CNOT (Controlled NOT), the reversible version of the XOR (`(a, b)` $\mapsto$ `(a, a⊕b)`). It is self inverse and can be built up with Fredkin gates.

The generalization of the CNOT is the Toffoli gate, it is a "double controlled NOT" (`(a, b, c)` $\mapsto$ `(a, b, c⊕(a∧b))`) and is self inverse.

All these gates are shown in Figure 2.

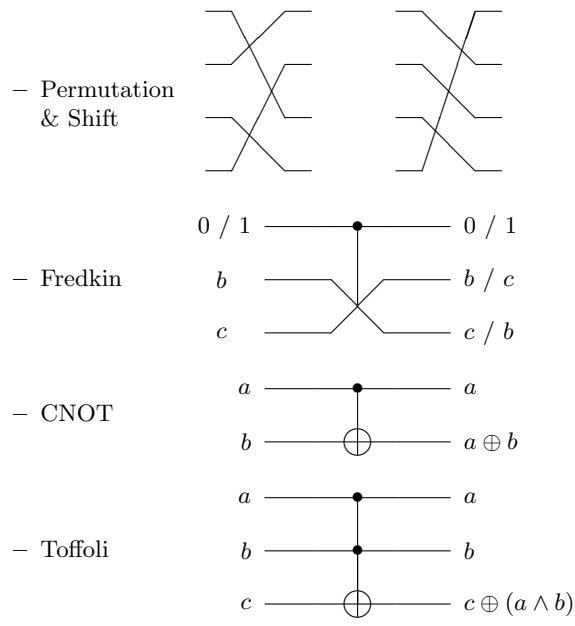


Fig. 2. Basic reversible gates

A polynomial basis multiplier, built up with reversible gates can be found in Figure 3. There are $n = 5$ steps required, each step needs

- 2 shift(n) operations;
- wgt($f(x)$) $- 2 = 1$ CNOT gates (the feedback operation) and
- $n = 5$ Toffoli gates.

The normal basis multiplier suggested by Massey and Omura [11], modified for reversible gates, is shown in Figure 4. There are $n = 5$ steps required, each step needs

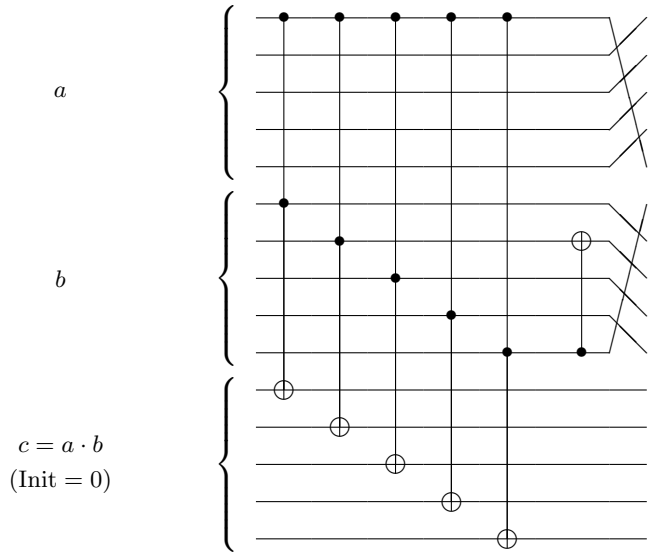


Fig. 3. A polynomial basis multiplier modulo $f(x) = x^5 + x^2 + 1$

– 3 shift(n) operations and
– "normal basis complexity ($f(x)$)" = 9 Toffoli gates.

There are other realizations of normal basis multipliers, but the "normal basis complexity", as defined in [13], is a lower bound for the number of gates needed. This bound is for optimal normal bases of $\mathbb{F}_{2^n}$ equal to $2n - 1$. In most field extensions such a basis does not exist and in some cases the best known normal basis of $\mathbb{F}_{2^n}$ is not much smaller than $n^2/2$. More details in this topic can be found in [6,8].

2 Redundant Representation of Finite Fields

The representation of $\mathbb{F}_{2^n}$ given in this section can perfectly be used in reversible circuits; but the representation can as well be used for very efficient classical circuits.

The main reason to use a normal basis is the easy procedure for squaring as a cyclic shift. The advantage of a polynomial basis is the easy realization of the multiplication as linear feedback shift register.

A representation that merges these two advantages is the following:

Theorem 1. *Let $m \in \mathbb{N}$ be minimal with $x^m - 1 \in \mathbb{F}_2[x]$ has an irreducible factor $f(x)$ of degree n; let $\alpha \in \mathbb{F}_{2^n}$ be a zero of $f(x)$. Then the elements of $\mathbb{F}_{2^n}$ can be represented as $\mathbb{F}_2$-vectors of size m according to the following embedding:*

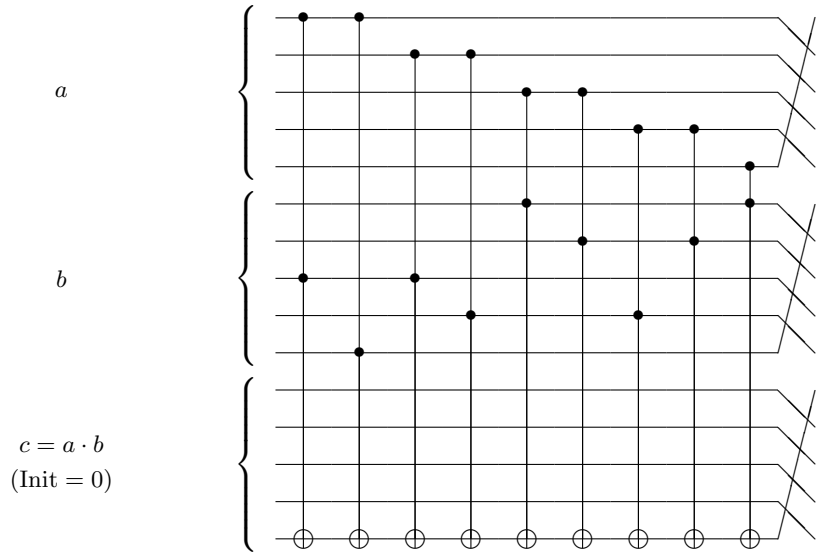


Fig. 4. The Massey-Omura normal basis multiplier with $f(x) = x^5 + x^4 + x^2 + x + 1$

$$
\begin{array}{lccccl}
\mathbb{F}_2[x]\Big/f(x) & \simeq & \mathbb{F}_2[\alpha] & \hookrightarrow & \mathbb{F}_2[x]\Big/(x^m-1) & \\
\phi: & \displaystyle\sum_{i=0}^{n-1} a_i \cdot \alpha^i & \mapsto & \displaystyle\sum_{i=0}^{n-1} a_i \cdot x^i & \hat{=} (a_0, \ldots, a_{n-1}, 0, \ldots, 0) & \\
\overline{\phi}: & \displaystyle\sum_{i=0}^{m-1} b_i \cdot \alpha^i & \hookleftarrow & \displaystyle\sum_{i=0}^{m-1} b_i \cdot x^i & \hat{=} \quad (b_0, \ldots, b_{m-1})\,. &
\end{array}
$$

It holds:

(a) $\overline{\phi}(\phi(a) + \phi(b)) = a + b \quad$ *for* $a, b \in \mathbb{F}_2[\alpha]$,
(b) $\overline{\phi}(\phi(a) \cdot \phi(b)) = a \cdot b \quad$ *for* $a, b \in \mathbb{F}_2[\alpha]$.

Proof. Property (a) obviously holds.
To prove (b), note that $f(x) \mid (x^m - 1)$ and thus $\alpha^m = 1$. ∎

The arithmetic in $\mathbb{F}_2[x]\Big/(x^{n+1}+1)$, can be performed as follows:

- Addition: Is the XOR of the vectors.
- Multiplication with x: Is a cyclic shift.
  With $b := \displaystyle\sum_{i=0}^{m-1} b_i \cdot x^i$ it holds: $\begin{array}{c} b \;\hat{=}\, (b_0, b_1, \ldots, b_{m-1}) \\ \Rightarrow x \cdot b \,\hat{=}\, (b_{m-1}, b_0, \ldots, b_{m-2}). \end{array}$
- Multiplication: Is performed with an LFSR with trivial feedback polynomial $x^m - 1$.

– Squaring: Is a permutation ("stretching").
(Note m is odd, because of m being minimal with $f(x) \mid (x^m - 1)$.) Let $b := \sum_{i=0}^{m-1} b_i \cdot x^i$, then

$$b^2 = \sum_{i=0}^{m-1} b_i \cdot x^{2\,i} = \sum_{i=0}^{(m-1)/2} b_i \cdot x^{2\,i} + \sum_{i=(m+1)/2}^{m-1} b_i \cdot x^{2\,i-m}.$$

Written as vectors this is:

$$\begin{aligned} b &\mathrel{\hat{=}} (b_0, b_1, b_2, \ldots, b_{m-1}) \\ \Rightarrow b^2 &\mathrel{\hat{=}} (b_0, b_{(m+1)/2}, b_1, b_{(m+3)/2}, b_2, \ldots, b_{m-1}, b_{(m-1)/2}). \end{aligned}$$

Example 1. The elements of the field $\mathbb{F}_{2^4}$ can be represented as vectors of length 5 according to the factorization of $x^5 + 1 \in \mathbb{F}_2[x]$ to $x^5 + 1 = (x + 1)(x^4 + x^3 + x^2 + x + 1)$. Let α be a zero of $x^4 + x^3 + x^2 + x + 1$, then $(1 + \alpha^3)^3$ can be calculated as follows:

$$\begin{aligned} \mathbb{F}_2[\alpha] &\hookrightarrow \mathbb{F}_2[x \,/\, (x^5 + 1)] \\ 1 + \alpha^3 &\mathrel{\hat{=}} (1, 0, 0, 1, 0) \\ (1 + \alpha^3)^2 &\mathrel{\hat{=}} (1, 1, 0, 0, 0) \quad \text{(by stretching)} \\ (1 + \alpha^3)^2 \cdot (1 + \alpha^3) &\mathrel{\hat{=}} (1, 1, 0, 0, 0) \oplus (0, 0, 0, 1, 1) \\ &\mathrel{\hat{=}} (1, 1, 0, 1, 1) \quad \text{(with } \alpha^4 = \alpha^3 + \alpha^2 + \alpha + 1 \\ &\qquad\qquad\qquad\qquad\quad \text{this reduces to)} \\ \alpha^2 &\mathrel{\hat{=}} (1, 1, 0, 1, 1). \end{aligned}$$

In the appendix a list of the minimal required length m of the redundant representation is given for $n \leq 250$ and for primes $n \leq 2000$.

3 Multiplication with a Fixed Element

For crypto systems based on a discrete logarithm problem in $\mathbb{F}_{2^n}$ exponentiation of one fixed element $a \in \mathbb{F}_{2^n}$ is one of the operations required. This is an operation perfectly suited to reversible computing when squaring is a permutation. The multiplication with a is a linear mapping and can be performed without any intermediate results that need to be deleted.

One way to generate a reversible implementation of a linear mapping (represented as multiplication $\phi(a) \mapsto A \cdot \phi(a)$ with A an $m \times m$ matrix and $\phi(a)$ a vector of size m) is to decompose A into $A = P \cdot L \cdot U$ with P a permutation matrix, L a lower triangular matrix and U an upper triangular matrix.

For the multiplication $U \cdot \phi(a)$ first calculate the first component by adding the required components to it (first row of U). After this step one bit of the result is stored in the first component – the previous value is lost, but not needed any more because of the trinagular structere of U. Proceeding with the other components of $\phi(a)$ in the same way gives $U \cdot \phi(a)$ without any intermediate

result to be deleted. The number of CNOT gates required is the weight of $U - I_m$, where I_m denotes the unity matrix of size m.

The multiplication with L is performed in the same way, but the resulting bits are calculated in the reverse order.

In the rest of this section we give some examples for normal basis multiplication and the multiplication in the corresponding redundant representation with reversible gates according to the decomposition of matrices.

Example 2. For the smaller examples the decomposition of the matrices is given, for the larger ones we restrict ourself to the complexity only.

- $\mathbb{F}_{2^4}$:
  Let α be a zero of $x^4 + x^3 + x^2 + x + 1$, then α generates a normal basis with the multiplication matrix

$$A_4 := \begin{pmatrix} 0\,1\,0\,0 \\ 0\,0\,0\,1 \\ 1\,1\,1\,1 \\ 0\,0\,1\,0 \end{pmatrix}.$$

  Then $\alpha + 1$ is a primitive element and the multiplication with $A_4 + I_4$ decomposes as follows:

$$A_4 + I_4 = \begin{pmatrix} 1\,0\,0\,0 \\ 0\,1\,0\,0 \\ 0\,0\,0\,1 \\ 0\,0\,1\,0 \end{pmatrix} \cdot \begin{pmatrix} 1\,0\,0\,0 \\ 0\,1\,0\,0 \\ 0\,0\,1\,0 \\ 1\,0\,0\,1 \end{pmatrix} \cdot \begin{pmatrix} 1\,1\,0\,0 \\ 0\,1\,0\,1 \\ 0\,0\,1\,1 \\ 0\,0\,0\,1 \end{pmatrix}.$$

  This decomposition results in a multiplication circuit with $1 + 3 = 4$ CNOT gates and 1 permutation of two elements.

  For the redundant representation $m = 5$ (note: $x^5 = (x + 1)(x^4 + x^3 + x^2 + x + 1)$). The matrix $R_4 \in \mathbb{F}_2^{5\times 5}$ corresponding to multiplication with x has to perform a cyclic shift and thus is the circulant matrix with first row $(0, 1, 0, 0, 0)$. The element $1 + x + x^2$ is primitive, and the decomposition of the corresponding matrix is:

$$I_5 + R_4 + R_4^2 = \begin{pmatrix} 1\,0\,0\,0\,0 \\ 0\,1\,0\,0\,0 \\ 0\,0\,1\,0\,0 \\ 0\,0\,0\,0\,1 \\ 0\,0\,0\,1\,0 \end{pmatrix} \cdot \begin{pmatrix} 1\,0\,0\,0\,0 \\ 0\,1\,0\,0\,0 \\ 0\,0\,1\,0\,0 \\ 1\,0\,1\,1\,0 \\ 1\,1\,0\,0\,1 \end{pmatrix} \cdot \begin{pmatrix} 1\,1\,1\,0\,0 \\ 0\,1\,1\,1\,0 \\ 0\,0\,1\,1\,1 \\ 0\,0\,0\,1\,0 \\ 0\,0\,0\,0\,1 \end{pmatrix}.$$

  Here the multiplication circuit requires $4 + 6 = 10$ CNOT gates and 1 permutation of two elements.

– $\mathbb{F}_{2^6}$:
In this field an optimal normal basis exists with the multiplication matrix:

$$A_6 := \begin{pmatrix} 0&1&0&0&0&0 \\ 1&0&0&0&1&0 \\ 0&0&0&1&1&0 \\ 0&0&1&0&0&1 \\ 0&1&1&0&0&0 \\ 0&0&0&1&0&1 \end{pmatrix}$$

The corresponding field element is primitive and A_6 decomposes to:

$$A_6 = \begin{pmatrix} 0&1&0&0&0&0 \\ 1&0&0&0&0&0 \\ 0&0&0&1&0&0 \\ 0&0&1&0&0&0 \\ 0&0&0&0&0&1 \\ 0&0&0&0&1&0 \end{pmatrix} \cdot \begin{pmatrix} 1&0&0&0&0&0 \\ 0&1&0&0&0&0 \\ 0&0&1&0&0&0 \\ 0&0&0&1&0&0 \\ 0&0&0&1&1&0 \\ 0&1&1&0&0&1 \end{pmatrix} \cdot \begin{pmatrix} 1&0&0&0&1&0 \\ 0&1&0&0&0&0 \\ 0&0&1&0&0&1 \\ 0&0&0&1&1&0 \\ 0&0&0&0&1&1 \\ 0&0&0&0&0&1 \end{pmatrix},$$

giving a reversible realization with $3+4 = 7$ CNOT gates and 3 permutations of two elements.

For the redundant representation $m = 9$ (note: $x^9 + 1 = (x + 1)(x^2 + x + 1)(x^6 + x^3 + 1)$). The element $1 + x + x^3$ is primitive, and the decomposition of the corresponding matrix is:

$$I_9 + R_6 + R_6^3 = \begin{pmatrix} 1&0&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0&0 \\ 0&0&0&0&1&0&0&0&0 \\ 0&0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&0&0&1 \end{pmatrix} \cdot \begin{pmatrix} 1&0&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0&0 \\ 0&0&0&0&1&0&0&0&0 \\ 0&0&0&0&0&1&0&0&0 \\ 1&1&1&0&1&0&1&0&0 \\ 0&1&1&1&0&1&0&1&0 \\ 1&1&0&1&0&0&1&0&1 \end{pmatrix} \cdot \begin{pmatrix} 1&1&0&1&0&1&0&0&0 \\ 0&1&1&0&1&0&1&0&0 \\ 0&0&1&1&0&1&0&1&0 \\ 0&0&0&1&1&0&1&0&0 \\ 0&0&0&0&1&1&0&1&0 \\ 0&0&0&0&0&1&1&0&1 \\ 0&0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&0&0&1 \end{pmatrix}.$$

Here the multiplication circuit requires $12 + 12 = 24$ CNOT gates and no permutation.

– $\mathbb{F}_{2^{54}}$:
In $\mathbf{F}_{2^{54}}$ a good normal basis (with complexity 209) exists. The generator α is not primitive, thus we choose the primitive Element: $1 + \alpha$. The decomposition of the corresponding matrix gives us a circuit with $236 + 255 = 491$ CNOT gates and a very irregular permutation.

The redundant representation with $m = 81$ and the primitive element $x + x^3 + x^4$ gives a circuit with $135 + 159 = 294$ CNOT gates and a very regular permutation, a cyclic shift on all but 3 elements.

- $\mathbb{F}_{2^{121}}$:
  In $\mathbb{F}_{2^{121}}$ a good normal basis (with complexity 705) exists. The generator α is primitive and the decomposition of the corresponding matrix gives us a circuit with $1183+1126 = 2309$ CNOT gates and a very irregular permutation.

  The redundant representation with $m = 727$ and the primitive element $x + x^2 + x^3$ gives a circuit with $968+550 = 1518$ CNOT gates and a very regular permutation, close to a cyclic shift.

- $\mathbb{F}_{2^{239}}$:
  In $\mathbb{F}_{2^{239}}$ a good normal basis (with complexity 477) exists. The generator α is primitive and the decomposition of the corresponding matrix gives us a circuit with $233 + 234 = 467$ CNOT gates and a very irregular permutation.

  The redundant representation with $m = 479$ and the primitive element $x + x^2 + x^3$ gives a circuit with $637+955 = 1592$ CNOT gates and a very regular permutation, close to a cyclic shift.

- $\mathbb{F}_{2^{240}}$:
  In $\mathbb{F}_{2^{240}}$ no good normal basis exists. We chose the best we found, with complexity 28433. The generator α is primitive and the decomposition of the corresponding matrix gives us a circuit with $14213 + 14370 = 28583$ CNOT gates and a very irregular permutation.

  The redundant representation with $m = 1067$ and the primitive element $1 + x + x^2$ gives a circuit with $1420 + 2130 = 3550$ CNOT gates and a very regular permutation, close to a cyclic shift.

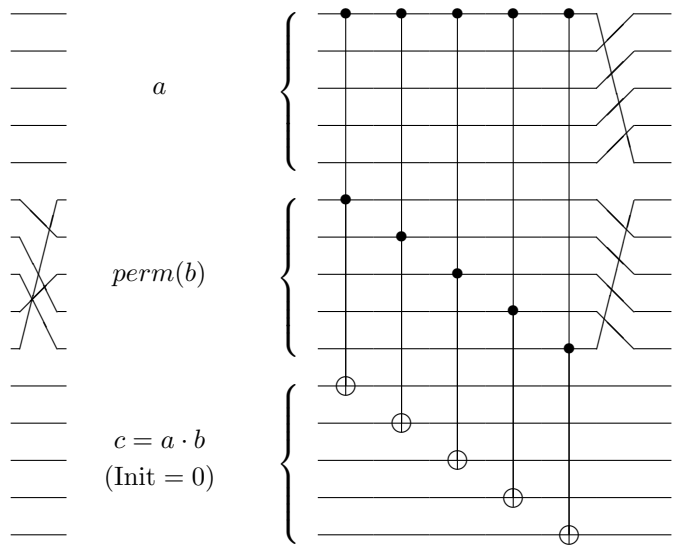
If a good normal bases exists in a field extension, it depends very much on the degree of redundancy required, if the normal basis representation or the redundant representation is better. If an optimal normal basis of type 1 (see. [13]) exists for the extension degree n, the redundant representation with $m = n+1$ is the best choice for implementation; if an optimal normal basis of type 2 (see. [13]) exists, the best redundant representation is with $m = 2n - 1$ and the normal basis multiplication (with complexity $2n - 1$) is the better choice.

If no good normal basis exists in the field in question even a high degree of redundancy will result in a better performance than a normal basis multiplier.

4 General Multiplication

The general multiplication (with two variable inputs) can be realized with reversible gates in a straight forward manner. There are exactly m Toffoli gates and 2 cyclic shifts of m signals needed. It corresponds directly to a LFSR with trivial feedback polynomial.

The major problem of any normal basis multiplier is the irregular structure. In hardware it results in additional area needed for wireing, in software unregular access to the bits causes additional operations. With the redundant representation these problems do not occure at all. The highly regular structure can be seen best in some example: The field $\mathbb{F}_{2^4}$ is represented as $\mathbb{F}_2[x]/(x^5 - x)$:



The corresponding normal basis multiplier needs "normal basis complexity $(f(x))$" many Toffoli gates, in this example this is 9. The permutation of the input b seems to reduce the advantage of the redundant representation; in cryptography in most cases an exponentiation is required, and thus the permutation has to be performed only once and not for each multiplication.

In this setting the redundant representation has often a better performance than a normal basis representation if the number of gates is the measure to be used. If the regularity of the design is taken into account the advantage is even more pronounced.

5 Conclusion

The presented redundant representation of finite extension fields via roots of unity joins the two good properties of normal and polynomial bases. On the one hand squaring can be performed by a simple and very structured permutation – a stretching; on the other hand multiplication can be performed with an LFSR with trivial feedback polynomial.

The price to pay is the additional place required for storage of the redundancy. The level of redundancy depends very much on the degree of the field and in many cases it is a perfect choice for exponentiation.

A Degree of Redundancy

In the following table for all fields $\mathbf{F}_{2^n}$ with $n \leq 250$ and extension degrees with $n \leq 2000$ beeing a prime, the smallest degree of redundancy m is given, that allows a representation with roots of unity. In some cases even the field $\mathbf{F}_{2^{n_1}} \supset \mathbf{F}_{2^n}$ can be represented with the smallest m-th roots of unity where $\mathbf{F}_{2^n}$ can be embedded.

n	n_1	m
2	2	3
3	3	7
4	4	5
5	10	11
6	6	9
7	28	29
8	8	17
9	18	19
10	10	11
11	11	23
12	12	13
13	52	53
14	28	29
15	60	61
16	48	97
17	51	103
18	18	19
19	95	191
20	20	25
21	21	49
22	66	67
23	23	47
24	48	97
25	100	101
26	52	53
27	54	81
28	28	29
29	58	59
30	60	61
31	155	311
32	96	193
33	66	67
34	68	137
35	35	71
36	36	37
37	148	149
38	76	229
39	39	79
40	40	187
41	82	83
42	42	147
43	172	173
44	44	115
45	180	181
46	138	139
47	94	283
48	48	97
49	196	197
50	100	101
51	51	103
52	52	53
53	106	107
54	54	81
55	110	121
56	224	449
57	342	361
58	58	59
59	708	709
60	60	61
61	183	367
62	372	373
63	378	379
64	64	641
65	130	131
66	66	67
67	268	269
68	68	137
69	138	139
70	210	211
71	284	569
72	72	323
73	292	293
74	148	149
75	300	707
76	76	229
77	231	463
78	156	169
79	316	317
80	240	1067
81	162	163
82	82	83
83	83	167
84	84	203
85	340	1021
86	172	173
87	348	349
88	88	353
89	178	179
90	180	181
91	546	547
92	92	235
93	372	373
94	94	283
95	95	191
96	96	193
97	388	389
98	196	197
99	99	199
100	100	101
101	303	607
102	102	307
103	618	619
104	104	901
105	210	211
106	106	107
107	214	643
108	108	405
109	1090	1091
110	110	121
111	444	1043
112	224	449
113	226	227
114	342	361
115	460	461
116	116	295
117	117	937
118	708	709
119	119	239
120	120	1037
121	121	727
122	244	733
123	246	581
124	372	373
125	500	625
126	378	379
127	508	509
128	384	769
129	258	1033
130	130	131
131	131	263
132	132	299
133	532	1597
134	268	269
135	135	271
136	136	289
137	411	823
138	138	139
139	556	557
140	140	319
141	564	1129
142	284	569
143	858	859
144	144	577
145	290	649
146	292	293
147	147	343
148	148	149
149	298	1193
150	300	707
151	906	907
152	152	1217
153	612	613
154	154	617
155	155	311
156	156	169
157	1570	1571
158	316	317
159	318	749
160	480	2123

n	n_1	m
161	483	967
162	162	163
163	652	653
164	164	415
165	660	661
166	166	499
167	2338	2339
168	168	833
169	676	677
170	340	1021
171	342	361
172	172	173
173	346	347
174	348	349
175	700	701
176	704	1409
177	708	709
178	178	179
179	179	359
180	180	181
181	543	1087
182	546	547
183	183	367
184	184	799
185	370	1481
186	372	373
187	1122	1123
188	940	941
189	378	379
190	190	573
191	191	383
192	384	769
193	772	773
194	388	389
195	390	869
196	196	197
197	3546	3547
198	198	437
199	796	797
200	200	401
201	201	1609
202	404	809
203	812	841
204	204	409
205	820	821

n	n_1	m
206	618	619
207	828	829
208	1040	2081
209	418	419
210	210	211
211	1055	2111
212	212	535
213	852	853
214	214	643
215	1290	1291
216	648	1297
217	651	1303
218	1090	1091
219	876	877
220	220	575
221	442	443
222	444	1043
223	2676	2677
224	224	449
225	900	1919
226	226	227
227	908	5449
228	228	1603
229	916	2749
230	460	461
231	231	463
232	464	929
233	466	467
234	468	1007
235	940	941
236	708	709
237	237	1423
238	238	717
239	239	479
240	240	1067
241	723	1447
242	1210	1331
243	243	487
244	244	733
245	490	491
246	246	581
247	1482	1483
248	744	1489
249	249	1169
250	500	625

n	n_1	m
251	251	503
257	771	1543
263	526	1579
269	1076	2153
271	542	1627
277	1108	1109
281	562	563
283	566	1699
293	586	587
307	1228	1229
311	1866	1867
313	939	1879
317	8242	8243
331	1986	1987
337	3370	3371
347	2082	2083
349	3490	3491
353	2471	4943
359	359	719
367	734	2203
373	1492	1493
379	1516	4549
383	1532	4597
389	2334	9337
397	397	2383
401	1604	3209
409	1636	1637
419	419	839
421	842	4211
431	431	863
433	1732	1733
439	2195	4391
443	443	887
449	1796	3593
457	6855	13711
461	461	2767
463	5556	5557
467	2802	2803
479	958	3833
487	1948	1949
491	491	983
499	1996	1997
503	3018	3019
509	1018	1019
521	2084	16673

n	n_1	m
523	2615	5231
541	3246	9739
547	547	5471
557	557	3343
563	7882	7883
569	6828	6829
571	571	5711
577	2308	2309
587	8218	8219
593	1186	1187
599	2396	4793
601	601	3607
607	3642	3643
613	6130	6131
617	1234	4937
619	2476	2477
631	3155	6311
641	1282	1283
643	7716	7717
647	9058	9059
653	1306	1307
659	659	1319
661	1983	3967
673	2692	2693
677	2708	5417
683	683	1367
691	3455	6911
701	12618	12619
709	2836	2837
719	719	1439
727	2908	2909
733	7330	7331
739	2956	2957
743	743	1487
751	4506	4507
757	6056	12113
761	1522	1523
769	7690	7691
773	2319	4639
787	4722	4723
797	2391	4783
809	1618	1619
811	4055	8111
821	1642	6569
823	4115	8231

n	n_1	m	n	n_1	m	n	n_1	m	n	n_1	m
827	11578	11579	1097	7679	15359	1423	5692	5693	1693	1693	10159
829	8290	8291	1103	1103	2207	1427	8562	8563	1697	6788	13577
839	10068	10069	1109	4436	13309	1429	5716	5717	1699	6796	20389
853	3412	3413	1117	3351	6703	1433	4299	8599	1709	20508	20509
857	857	6857	1123	4492	4493	1439	1439	2879	1721	34420	34421
859	18898	18899	1129	4516	4517	1447	17364	34729	1723	1723	17231
863	5178	5179	1151	6906	6907	1451	1451	2903	1733	3466	3467
877	7016	14033	1153	12683	25367	1453	5812	5813	1741	19151	38303
881	15858	15859	1163	4652	37217	1459	1459	14591	1747	8735	17471
883	3532	3533	1171	7026	7027	1471	5884	23537	1753	7012	7013
887	1774	5323	1181	14172	14173	1481	2962	2963	1759	15831	31663
907	5442	5443	1187	4748	9497	1483	7415	14831	1777	7108	7109
911	911	1823	1193	3579	7159	1487	8922	8923	1783	21396	21397
919	3676	3677	1201	3603	7207	1489	14890	14891	1787	10722	10723
929	3716	7433	1213	14556	14557	1493	10451	20903	1789	17890	17891
937	2811	5623	1217	3651	29209	1499	1499	2999	1801	21612	21613
941	2823	5647	1223	1223	2447	1511	1511	3023	1811	1811	3623
947	5682	5683	1229	2458	2459	1523	3046	21323	1823	3646	10939
953	1906	1907	1231	9848	19697	1531	3062	9187	1831	10986	10987
967	7736	15473	1237	2474	19793	1543	6172	6173	1847	11082	11083
971	5826	5827	1249	12490	12491	1549	6196	6197	1861	18610	74441
977	1954	7817	1259	17626	17627	1553	4659	9319	1867	9335	18671
983	13762	13763	1277	25540	25541	1559	1559	3119	1871	1871	14969
991	8919	17839	1279	6395	12791	1567	6268	6269	1873	5619	11239
997	3988	3989	1283	2566	7699	1571	3142	12569	1877	1877	15017
1009	10090	10091	1289	2578	2579	1579	6316	6317	1879	7516	7517
1013	2026	2027	1291	6455	12911	1583	1583	3167	1889	3778	3779
1019	1019	2039	1297	5188	5189	1597	6388	6389	1901	3802	3803
1021	2042	10211	1301	26020	26021	1601	3202	3203	1907	11442	11443
1031	1031	2063	1303	10424	20849	1607	9642	9643	1913	13391	26783
1033	4132	4133	1307	2614	10457	1609	3218	16091	1931	1931	3863
1039	4156	4157	1319	3957	23743	1613	4839	9679	1933	23196	23197
1049	2098	2099	1321	1321	7927	1619	6476	12953	1949	35082	35083
1051	12612	12613	1327	5308	5309	1621	3242	29179	1951	42922	42923
1061	3183	6367	1361	1361	8167	1627	4881	29287	1973	3946	3947
1063	4252	4253	1367	1367	10937	1637	31103	62207	1979	39580	39581
1069	10690	10691	1373	16476	16477	1657	6628	26513	1987	7948	7949
1087	4348	4349	1381	1381	8287	1663	6652	6653	1993	1993	11959
1091	6546	6547	1399	12591	25183	1667	1667	13337	1997	87868	87869
1093	4372	4373	1409	2818	2819	1669	3338	16691	1999	9995	19991

References

1. ElGamal, T. (1985). *A public key cryptosystem and a signature scheme based on discrete logarithms.* IEEE Trans.Inform.Theory, **IT-31**, 469-472
2. Odlyzko, A.M. (1985). *Discrete logarithms in finite fields and their cryptographic significance.* Proc. of Eurocrypt'84, T.Beth, N.Cot, I.Ingemarsson (eds.), Springer LNCS 209, 224–314.

3. Agnew, G.B., Mullin, R.C., Onyszchuk, I.M., Vanstone, S.A. (1991). *An Implementation for a Fast Public Key Cryptosystem.* Journal of Cryptology, **3**, 63-79.
4. Bennet, C.H. (1982). *The thermodynamics of computation – a review.* International Journal of Theoretical Physics, 21, **12**, 905–940.
5. Beth, T., Gollmann, D. (1989). *Algorithm Engineering for Public Key Algorithms.* IEEE JSAC, **7**, 458–466.
6. Geiselmann, W., Gollmann, D. (1990). *VLSI design for exponentiation in GF(2^n).* Proc. of Auscrypt'90, Seberry, J., Pieprzyk, J. (eds.), Springer LNCS 453, 398–405.
7. Haining, F.; *Simple multiplication algorithms for a class of GF(2^n).* Electronics Letters, 28th March 1996; Vol 32, No 7, 636–637.
8. Hsu, I.S., Truong, T.K., Deutsch, L.J., Reed, I.S. (1988). *A Comparison of VLSI Architecture of Finite Field Multipliers Using Dual, Normal, or Standard Bases.* IEEE Trans. Comp., **C-37**, 735–739.
9. Kocher, P., Jaffe, J., Jun, B. (1999). *Differential Power Analysis.* Advances in Cryptology - CRYPTO'99, Wiener, M. (ed.). Springer, LNCS 1666, 388–397.
10. Koller, C.G., Athas, W.C., (1993). *Adiabatic Switching, Low Energy Computing, and the Physics of Storing and Erasing Information.* Proceedings of the Workshop on Physics and Computation, PhysCmp '92, IEEE Press.
11. Massey, J.L., Omura, J.K. (1981). *Computational method and apparatus for finite field arithmetic.* U.S. Patent application.
12. Merkle, R.C. (1993). *Reversible electronic logic using switches.* Nanotechnology, **4**, 21–40.
13. Mullin, R.C., Onyszchuk, I.M., Vanstone, S.A., Wilson, R.M. (1988) *Optimal Normal Bases in GF(p^n).* Discrete Applied Mathematics, **22**, 149–161.
14. Berlekamp, E.R. (1982). *Bit-Serial Reed-Solomon Encoders.* IEEE Trans.Inf.Th., **IT-28**, 869–874.
15. Lidl, R., Niederreiter, H. (1986). *Introduction to Finite Fields and Their Applications.* Cambridge University Press.
16. MacWilliams, F.J., Sloane, N.J.A. (1977). *The Theory of Error-Correcting Codes.* North Holland.