Journal of Siberian Federal University. Engineering & Technologies, 2019, 12(7), 802-809
~ ~ ~

УДК 512.643:621.391.7

Reconfigurable Parralel Multiple in the Galois Fields in Combination Logic

Timur A. Zubov,
Vitaly V. Sukhotin, Anton V. Khnykin*,
Andrey V. Mishurov and Alexander A. Gorchakovsky
Siberian Federal University
79 Svobodny, Krasnoyarsk, 660041, Russia

Received 12.06.2019, received in revised form 11.08.2019, accepted 17.09.2019

The concept of "multiplier" in Galois fields, which are widely used in cryptography and noise-resistant coding, is considered. The architecture of a parallel multiplier for the Galois fields is analyzed. Reconfigurable multiplier is constructed. It is shown that the use of this type of multiplier will significantly reduce the number of logic gates.

Keywords: multiplier, Galois fields, combinational logic, reconfigurable module, Bose Chaudhuri Hocquenghem Codes.

Citation: Zubov T.A., Sukhotin V.V., Khnykin A.V., Mishurov A.V., Gorchakovsky A.A. Reconfigurable parralel multiple in the Galois fields in combination logic, J. Sib. Fed. Univ. Eng. technol., 2019, 12(7), 802-809. DOI: 10.17516/1999-494X-0180.

Реконфигурируемый параллельный умножитель в конечных полях Галуа на комбинационной логике

Т.А. Зубов, В.В. Сухотин, А.В. Хныкин,
А.В. Мишуров, А.А. Горчаковский
Сибирский федеральный университет
Россия, 660041, Красноярск, пр. Свободный, 79

Рассмотрено понятие «умножитель» в конечных полях Галуа, имеющих широкое применение в криптографии и помехоустойчивом кодировании. Проанализирована архитектура параллельного умножителя над полями Галуа. Проведено построение реконфигурируемого умножителя. Показано, что применение данного типа умножителя позволит значительно сократить число применяемых логических вентилей.

Ключевые слова: умножитель, поля Галуа, комбинационная логика, реконфигурируемый модуль, коды Боуза-Чоудхури-Хоквингема.

* Corresponding author E-mail address: akhnykin@sfu-kras.ru

Введение

В нашу жизнь очень глубоко проникли цифровые технологии – от гаджетов до систем передачи информации. Очень большое внимание уделяется развитию стандартов передачи информации DVB-S2 и DVB-S2X в части обеспечения помехоустойчивости и оптимизации структур умножителей, входящих в состав кодеров/декодеров. Применение достаточно сложных кодов приводит к увеличению количества структур умножителей над несколькими полями Галуа, увеличению времени обработки информации и неэффективного использования программируемых логических интегральных схем (ПЛИС). Для того чтобы свести к минимуму или исключить указанные недостатки, требуется создать реконфигурируемый умножитель с минимальным количеством вентилей. Рассмотрим возможность построения данного умножителя и сделаем соответствующие выводы.

1. Что такое умножитель

Арифметика в полях Галуа широко используется в криптографии и помехоустойчивом кодировании, в частности в кодах Боуза-Чоудхури-Хоквингема (БЧХ), относящихся к семейству циклических кодов [1].

Умножение двух величин в конечном двоичном поле Галуа степени m GF(2^m) представляется следующим образом [2]:

$$C(x) = A(x)B(x) \bmod P(x), \tag{1}$$

где $A(x) = a_{m-1}x^{m-1} + a_{m-1}x^{m-2} + \ldots + a_1x + a_0 = \sum_{i=0}^{m-1} a_i x^i$ – полином степени $m-1$,

$B(x) = b_{m-1}x^{m-1} + b_{m-1}x^{m-2} + \ldots + b_1x + b_0 = \sum_{i=0}^{m-1} b_i x^i$ – полином степени $m-1$,

$P(x) = p_m x^m + p_{m-1}x^{m-1} + \ldots + p_1x + p_0 = p_m x^m + \sum_{i=0}^{m-1} p_i x^i$ – неприводимый полином степени m,

порождающий поле GF(2^m).

В конечном поле имеется примитивный элемент $\alpha \in GF(2^m)$, степени которого порождают ненулевые элементы поля, т.е. $\beta = \alpha^i \in GF(2^m), 0 \le i \le 2^m - 2$. Элемент α является корнем неприводимого двоичного полинома $P(x)$, $P(\alpha) = 0$ [2, с. 81]. Умножение двух величин (1) представляется следующим образом:

$$S = A(\alpha)B(\alpha) = \left(\sum_{i=0}^{m-1} a_i \alpha^i\right)\left(\sum_{j=0}^{m-1} b_j \alpha^j\right) = \sum_{k=0}^{2m-1} s_k \alpha^k, \tag{2}$$

где

$$s_k = \sum_{i+i=k} a_i b_j \ , \ 0 \le i, j \le m-1, \ 0 \le k \le 2m-1. \tag{3}$$

Полная операция умножения (1) двух величин в конечном двоичном поле Галуа такова [3]:

$$C \triangleq \sum_{i=0}^{m-1} c_i a^i \equiv S \bmod P(a). \tag{4}$$

2. Архитектура параллельного умножителя над полями Галуа

Для аппаратной реализации выражения (1) и (2) представляются в матричной форме [4]:

$$C = d + Q^T e, \tag{5}$$

где Q – двоичная матрица остатков:

$$Q = \begin{bmatrix} \alpha^m \bmod P(\alpha) \\ \alpha^{m+1} \bmod P(\alpha) \\ \vdots \\ \alpha^{2m-1} \bmod P(\alpha) \end{bmatrix}, \tag{6}$$

$$d = LB, \tag{7}$$

$$e = UB, \tag{8}$$

L и U – матрицы Теплица:

$$L \triangleq \begin{bmatrix} a_0 & 0 & 0 & \dots & 0 \\ a_1 & a_1 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ a_{m-2} & a_{m-3} & \dots & a_0 & 0 \\ a_{m-1} & a_{m-2} & \dots & a_1 & a_0 \end{bmatrix}, \quad U \triangleq \begin{bmatrix} 0 & a_{m-1} & a_{m-2} & \dots & a_1 \\ 0 & 0 & a_{m-1} & \dots & a_2 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & a_{m-1} \end{bmatrix}. \tag{9}$$

Архитектура low complexity bit parallel (LCBP) умножителя над полем Галуа, основанного на формуле (8) и архитектуре Мастравито [5], показана на рис. 1 [4].

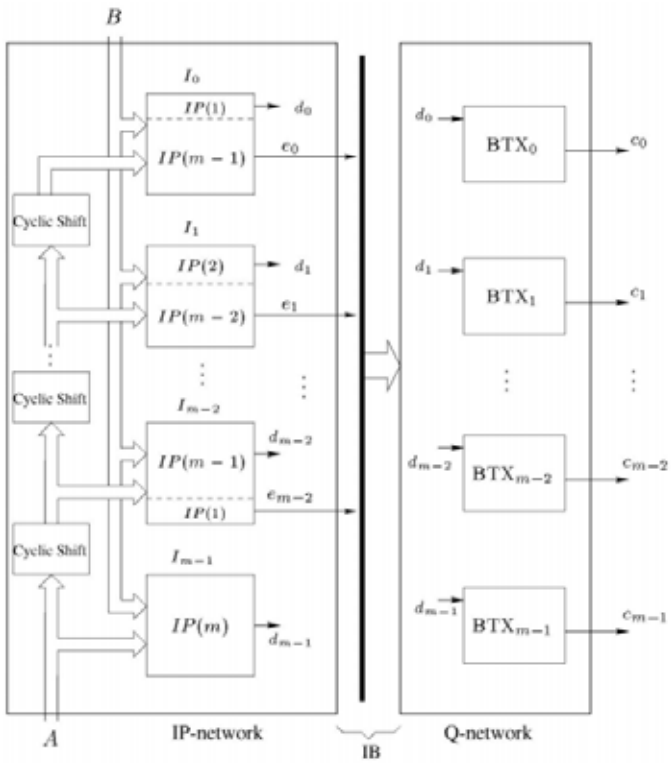

Рис. 1. Архитектура умножителя LCBP над полем GF(2^m)

Fig. 1. The architecture of the LCBP multiplier for the GF(2^m)

Архитектура состоит из двух частей: *IP*-область и *Q*-область. *IP*-область состоит из *m* *I*-блоков, вычисляющих вектора *d* и *e* по выражениям (6) и (7). *Q*-область состоит из *m* блоков $BTX_{0\ldots m-1}$, содержащих исключающие сумматоры XOR. Количество сумматоров BTX (i, $0 \le i \le m-1$) определяется количеством единиц в столбцах матрицы *Q*. Блок «Cyclic Shift» сдвигает старший разряд вектора на нулевую позицию, как показано на рис. 2.

Так, например, архитектура умножителя над полем GF(2^4), генерируемого полиномом $p(x) = x^4 + x + 1$, показана на рис. 3 [4].

Вычисление векторов *d* и *e* осуществляется при помощи полиномиального умножения в *IP*-области умножителя над полем GF(2^4) и выглядит следующим образом (рис. 4) [6].

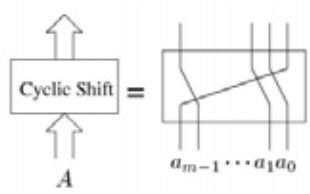

Рис. 2. Устройство блока «Cyclic Shift»

Fig. 2. Block «Cyclic Shift»

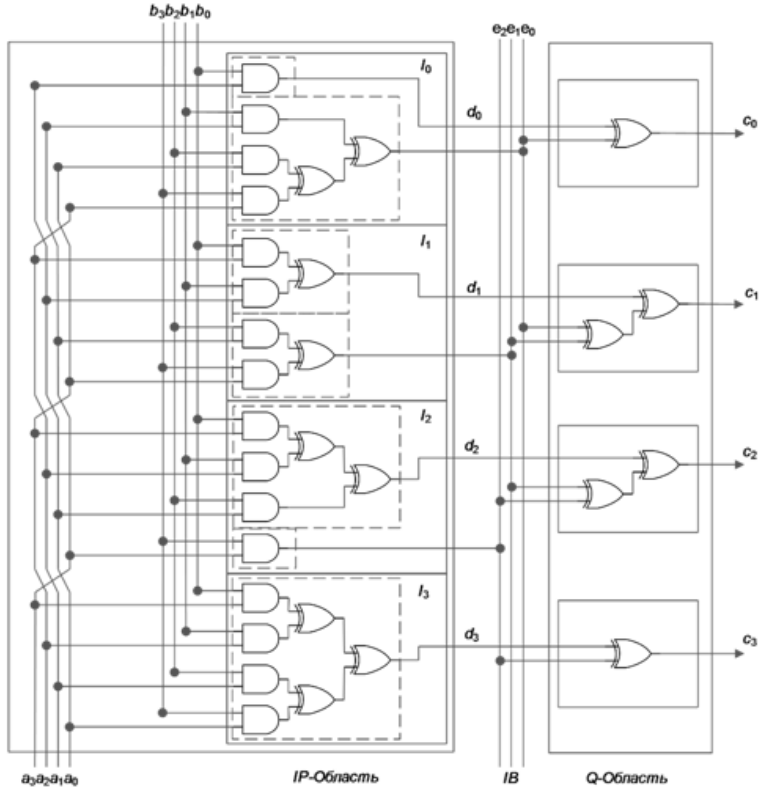

Рис. 3. Архитектура умножителя над полем GF(2^4)

Fig. 3. Multiplier architecture for GF(2^4)

	α^0	α	α^2	α^3	α^4	α^5	α^6
	A_0	A_1	A_2	A_3			
$\otimes$	B_0	B_1	B_2	B_3			
	A_0B_0	A_1B_0	A_2B_0	A_3B_0			
$\oplus$		A_0B_1	A_1B_1	A_2B_1	A_3B_1		
$\oplus$			A_0B_2	A_1B_2	A_2B_2	A_3B_2	
$\oplus$				A_0B_3	A_1B_3	A_2B_3	A_3B_3
	d_0	d_1	d_2	d_3	e_0	e_1	e_2

Рис. 4. Вычисление векторов d и e для поля GF(2^4)

Fig. 4. Calculation of vectors d and e for the field GF(2^4)

Количество блоков XOR и входные сигналы определяются матрицей Q, которая рассчитывается по формуле (6). Для умножителя над полем GF(2^4) матрица будет выглядеть так:

$$Q = \begin{matrix} d_0 & d_1 & d_2 & d_3 \end{matrix} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix} \begin{matrix} e_0 \\ e_1 \\ e_2 \end{matrix}. \tag{10}$$

Тогда величина C (5) будет вычислена следующим образом:

$$\begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} d_0 \oplus e_0 \\ d_1 \oplus e_0 \oplus e_1 \\ d_2 \oplus e_1 \oplus e_2 \\ d_3 \oplus e_2 \end{bmatrix}. \tag{11}$$

3. Построение параллельного реконфигурируемого умножителя

На практике не всегда используется умножение над одним полем Галуа, в частности, если рассматривать декодирования БЧХ(BCH) в стандарте DVB-S2X [7], то здесь используется умножение с тремя разными полями Галуа: GF(2^{16}) (нормальный FECFRAME, n = 64800), GF(2^{15}) (средний FECFRAME, n = 32400) и GF(2^{14}) (короткий FECFRAME, n = 16200), что требует наличие трех разных умножителей над тремя полями Галуа. Реализация каждого умножителя на основе структуры, показанной на рис. 1, достаточно затратная задача с точки зрения ресурсов. Только для *IP*-области потребуется m^2 логических блоков AND и $(m-1)^2$ логических блоков XOR, а для Q-области количество логических блоков XOR определяется количеством единиц в матрице Q. Количество вентилей для всех трех полей Галуа сведены в табл.

Как видно из данных таблицы, большая часть вентилей сосредоточена в *IP*-области. Чтобы построить реконфигурируемый умножитель, необходимо сформировать единую структуру для всех трех полей.

Перед тем как перейти к построению реконфигурируемого умножителя для стандарта DVB-S2X, рассмотрим возможность построения реконфигурируемого умножителя на двух элементарных полях. За основу возьмем архитектуру на рис. 3 с порождающим поле GF(2^4)

Таблица. Количество вентилей в умножителях над полями Галуа

Table. The number of logic gates in multipliers for the Galois fields

Поле	Порождающий полином $P(x)$	*IP*-Область		*Q*-Область
		AND, шт.	XOR, шт.	XOR, шт.
$GF(2^{16})$	$1+x^2+x^3+x^5+x^{16}$	256	225	71
$GF(2^{15})$	$1+x^2+x^3+x^5+x^{15}$	225	196	67
$GF(2^{14})$	$1+x+x^3+x^5+x^{14}$	196	169	62

полиномом $p(x) = x^4 + x + 1$ и к нему добавим $p(x) = x^3 + x + 1$, генерирующим $GF(2^3)$. Выбор данных полиномов связан с тем, что младшие члены полиномов близки или одинаковы, такую же схожесть имеют полиномы, приведенные в табл. Полиномиальное умножение для $GF(2^3)$ в *IP*-области для вычисления векторов *d* и *e* показано на рис. 5.

Матрица остатков для поля $GF(2^3)$, рассчитанная по формуле (6), выглядит так:

$$Q = \begin{matrix} d_0 & d_1 & d_2 \\ \end{matrix} \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \begin{matrix} e_0 \\ e_1 \end{matrix}. \tag{12}$$

Величина *C* (5) будет вычислена следующим образом:

$$\begin{bmatrix} c_0 \\ c_1 \\ c_2 \end{bmatrix} = \begin{bmatrix} d_0 \oplus e_0 \\ d_1 \oplus e_0 \oplus e_1 \\ d_2 \oplus e_1 \end{bmatrix}. \tag{13}$$

Сравнив полиномиальное умножение для $GF(2^3)$ и $GF(2^4)$ на рис. 3 и 5, можно увидеть, что полиномиальное умножение для $GF(2^3)$ можно осуществить в схеме, предназначенной для $GF(2^4)$ благодаря тому, что свертка – линейная операция. Прибегнув к обнулению старших разрядов *a* и *b* на входе и к линейному преобразованию элементов векторов *d* и *e* на выходе, можно показать умножение для $GF(2^3)$ в схеме $GF(2^4)$, что отображено на рис. 6.

Вектора *d'* и *e'* – преобразованные вектора *d* и *e*, адаптированные для $GF(2^3)$.

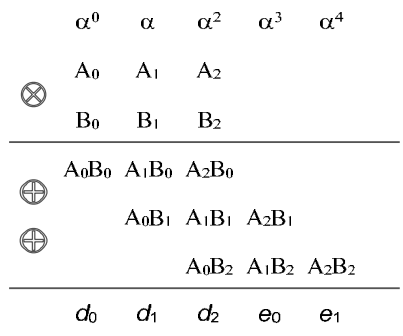

Рис. 5. Вычисление векторов *d* и *e* для поля $GF(2^3)$

Fig. 5. Calculation of vectors *d* and *e* for the $GF(2^3)$

	α^0	α	α^2	α^3	α^4	α^5	α^6
$\otimes$	A_0	A_1	A_2	0			
	B_0	B_1	B_2	0			
$\oplus$	A_0B_0	A_1B_0	A_2B_0	0			
$\oplus$		A_0B_1	A_1B_1	A_2B_1	0		
$\oplus$			A_0B_2	A_1B_2	A_2B_2	0	
				0	0	0	0
$GF(2^4)$	d_0	d_1	d_2	d_3	e_0	e_1	e_2
$GF(2^3)$	d_0	d_1	d_2	e_0	e_1	0	0
	d'_0	d'_1	d'_2	e'_0	e'_1	d'_3	e'_2

Рис. 6. Вычисление векторов *d* и *e* поля GF(2^3) в схеме, предназначенной для GF(2^4)

Fig. 6. Calculation of vectors *d* and *e* of the GF(2^3) in the scheme for GF(2^4)

Рассмотрев матрицы (10) и (11), можно увидеть, что матрица (11) является подматрицей (10), которая выделена в выражении:

$$Q' = \begin{matrix} d'_0 & d'_1 & d'_2 & 0 \end{matrix} \begin{bmatrix} \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} & \begin{matrix} 0 \\ 0 \end{matrix} \\ \begin{matrix} 0 & 0 & 1 \end{matrix} & 1 \end{bmatrix} \begin{matrix} e'_0 \\ e'_1 \\ 0 \end{matrix}. \tag{14}$$

Величина *C* будет следующей:

$$\begin{bmatrix} c'_0 \\ c'_1 \\ c'_2 \\ c'_3 \end{bmatrix} = \begin{bmatrix} d'_0 \oplus e'_0 \\ d'_1 \oplus e'_0 \oplus e'_1 \\ d'_2 \oplus e'_1 \oplus e'_2 \\ d'_3 \oplus e'_2 \end{bmatrix} = \begin{bmatrix} d'_0 \oplus e'_0 \\ d'_1 \oplus e'_0 \oplus e'_1 \\ d'_2 \oplus e'_1 \oplus 0 \\ 0 \oplus 0 \end{bmatrix} = \begin{bmatrix} d'_0 \oplus e'_0 \\ d'_1 \oplus e'_0 \oplus e'_1 \\ d'_2 \oplus e'_1 \\ 0 \end{bmatrix} = \begin{bmatrix} C_{GF(2^3)} \\ 0 \end{bmatrix}. \tag{15}$$

Таким образом, блоки BTX_i ($0 \le i \le 3$) остаются без внесения изменений и реконфигурируемая архитектура будет выглядеть, как это показано на рис. 7.

На рис. 7 видно, что количество умножителей AND и исключающих сумматоров в *IP*-области, ограничиваясь старшим полем, до значений 4^2 и 3^2 соответственно вместо 4^2+3^2 и 3^2+2^2 для двух отдельных архитектур, уменьшено.

Заключение

Реконфигурируемый умножитель над полями Галуа сформирован. Построенная реконфигурируемая архитектура параллельного умножителя над двумя полями Галуа GF(2^4) и GF(2^3) позволяет сократить количество умножителей AND и исключающих сумматоров в *IP*-области, ограничиваясь старшим полем, до значений 4^2 и 3^2 соответственно вместо 4^2+3^2 и 3^2+2^2 для двух отдельных архитектур. Также перестановкой элементов векторов *d* и *e* и сопоставлением расположения ненулевых элементов матриц остатков *Q* можно минимизировать количество исключающих сумматоров XOR в *Q*-области. Предложенный подход к построению реконфигурируе-

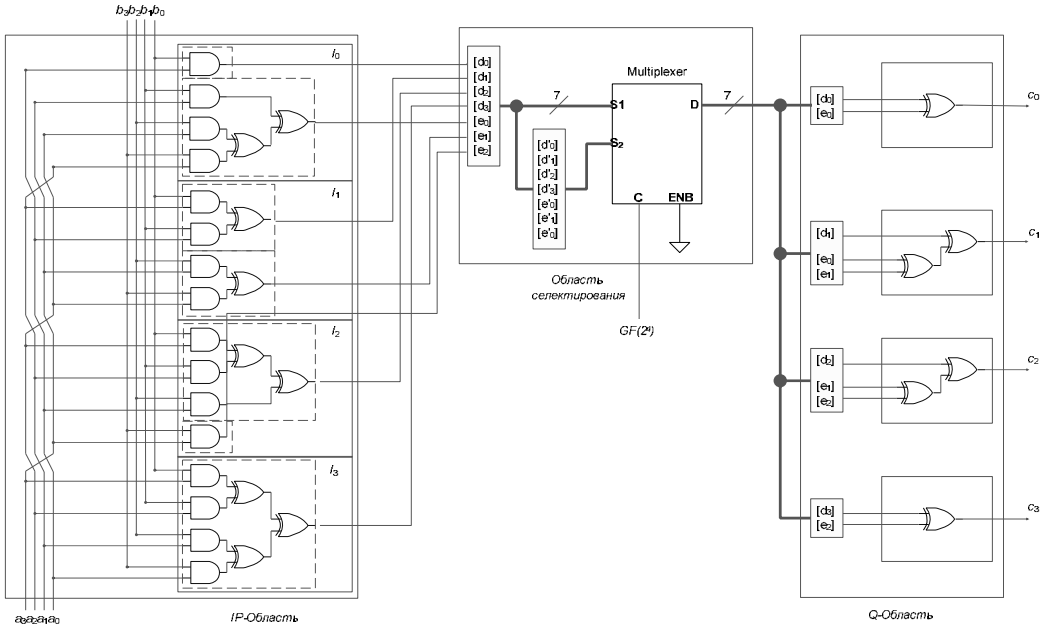

Рис. 7. Реконфигурируемая архитектура умножителя над полями GF(2^4) и GF(2^3)

Fig. 7. Reconfigurable multiplier architecture for GF(2^4) and GF(2^3)

мого умножителя, исходя из принятых условий, возможно распространить для формирования такого в стандарте DVB-S2X.

Список литературы

[1] Сагалович Ю.Л. *Введение в алгебраические коды*. М.: МФТИ, 2007. 262 с. [Sagalovich Yu.L. *Introduction to algebraic codes*, Moscow, MIPT, 2007, 262 p. (in Russian)]

[2] Mathew J., Jabir A.M., Rahaman H., Pradhan D.K. Single error correctable bit parallel multipliers over GF(2^m), *IET Computers & Digital Techniques*, 2009, 3(3), 281–288.

[3] Морелос-Сарагоса Р. *Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение*. М.: Техносфера, 2005. 320 с. [Morelos-Zaragoza R. *The art of noise-tolerant coding. Methods, algorithms, application*, Moscow, Technosphere, 2005, 320 p. (in Russian)]

[4] Reyhani-Masoleh A., Anwar Hasan M. Low Complexity Bit Parallel Architectures for Polynomial Basis Multiplication over GF(2^m), *IEEE Transactions on Computers,* 2004, 53(8), 945–959.

[5] Halbutogullari A., Koc C. Mastrovito Multiplier for General Inrreducible Polynominals, *IEEE Transactions on Computers*, 2000, 49(5), 503–518.

[6] Lee C.Y., Lu E.H. Lee J.Y. Bit-Parallel Systolic Multipliers for GF(2^m) Fields Defined by All-One and Equally Spaced Polynomials, *IEEE Transactions on Computers*, 2001, 50(5), 385–393.

[7] ETSI. Digital video broadcasting (DVB). Second generation framing structure, channel coding and modulation systems for broadcasting, interactive services, news gathering and other broadband satellite applications; Part 2: DVB-S2 Extensions (DVB-S2X): EN 302 307-2 V1.3.1, 2014.