Fast Systematic Encoding of Quasi-Cyclic Codes Using the Chinese Remainder Theorem

Pavel Panteleev
Faculty of Mechanics and Mathematics
Lomonosov Moscow State University
GSP-1, Leninskiye Gory, Moscow, 119991, Russian Federation
Email: panteleev@intsys.msu.ru

***Abstract*—Quasi-cyclic (QC) codes are a wide class of error-correcting codes possessing nice theoretical properties and having many practical applications. This paper provides a new approach to the problem of efficient encoding of QC codes based on the Chinese remainder theorem (CRT). We present a number of fast systematic CRT-based encoding algorithms that have superior asymptotic complexity than the previous methods based on shift registers. We also consider the encoding problem for QC low-density parity-check (LDPC) codes. In the special case when the parity part of a sparse parity-check QC matrix has a QC generalized inverse we propose a systematic CRT-based encoding algorithm that can exploit the parity-check matrix sparseness. We also give necessary and sufficient conditions when a QC matrix over an arbitrary field has a QC generalized inverse of the same circulant size.**

I. Introduction

Quasi-cyclic (QC) codes introduced by Townsend and Weldon [1] are an important class of linear codes having reach algebraic structure and widely used in applications. A linear (N, K)-code is said to be a QC code of index n, where $n \mid N$, if the right cyclic shift by n positions of any codeword is also a codeword. Thus cyclic codes are just a special case of QC codes when $n = 1$. It is known [2] that in the class of QC codes there are asymptotically good codes meeting a Gilbert-Varshamov type bound. At the same time, the question whether there exists an asymptotically good class of cyclic codes is a long-standing problem [3].

Since the reinvention of the capacity-approaching low-density parity-check (LDPC) codes in 1990s, first introduced by Gallager in 1960s [4], a subclass of QC codes with sparse parity-check matrices called QC LDPC codes has gained significant attention [5]. The quasi-cyclic structure of these codes makes them particularly convenient for encoding and decoding.

In this paper we address the problem of efficient encoding of QC codes. It is very well known that QC codes can be encoded by multiplying of an information vector by a generator QC matrix, which can be implemented in hardware using shift registers (see [6] for a good reference on this topic). Despite the regular structure of such algorithms, which simplifies the hardware implementation, their bit complexity is still proportional to the number of non-zero elements in the generator matrix. This makes them less attractive for high-throughput applications in modern communications and storage systems. Thus a development of faster encoding methods for QC and QC LDPC codes is of significant theoretical and practical importance.

In fact, a vector by a QC matrix multiplication can be implemented much more efficiently if one uses the polynomial representation of QC matrices. Suppose we have an $m\ell \times n\ell$ QC matrix over $\mathbb{F}_q$ consisting of $m \times n$ circulant submatrices of size $\ell \times \ell$. It can be represented [7], [8] as the polynomial $m \times n$ matrix with coefficients from the ring $\mathbb{F}_q^{\langle \ell \rangle} = \mathbb{F}_q[x]/(x^\ell - 1)$. Thus we need mn multiplications[1] in the ring $\mathbb{F}_q^{\langle \ell \rangle}$ to multiply by this matrix. A straightforward approach to implement multiplication in $\mathbb{F}_q^{\langle \ell \rangle}$ leads to $O(\ell^2)$ arithmetic operations in the field $\mathbb{F}_q$ but using the classical Fast Fourier Transform (FFT) based polynomial multiplication algorithms[2] [9, Chapter 8] it is possible to use only $O(\ell \log \ell \log\log \ell)$ field operations. Hence the total complexity of the FFT-based multiplication by an $m\ell \times n\ell$ QC matrix is $O(mn\ell \log \ell \log\log \ell)$ arithmetic operations in the field $\mathbb{F}_q$. Some other types of asymptotically fast algorithms for QC matrix multiplication were considered in [10] in the context of the McEliece cryptosystem.

Despite good asymptotic properties of the FFT-based and other asymptotically fast polynomial multiplication algorithms, their complexity for finite values of ℓ is not so good and can be even worse than in the straightforward implementation [9, Section 9.7]. In this paper we propose another approach to this problem. We use the Chinese Remainder Theorem (CRT) to represent all the polynomials involved in the QC matrix multiplication as elements of the product:

$$\mathbb{F}_{q_1} \times \cdots \times \mathbb{F}_{q_s}. \tag{1}$$

This CRT representation allows us to find the product of polynomials in $\mathbb{F}_q^{\langle \ell \rangle}$ as the pointwise product in (1), which is usually much simpler. After the QC matrix multiplication is done we transform all the output data back into the original representation. The proposed algorithm can be viewed as a generalization of the Winograd polynomial multiplication algorithm [11, Chapter VI]. Such algorithms that use the CRT representation for fast calculations are quite common in computer algebra and called *modular algorithms* [9, Chapter 5].

[1] The addition in the ring $\mathbb{F}_q^{\langle \ell \rangle}$ has the complexity of $O(\ell)$ and is not taken into account.

[2] To reduce the result of polynomial multiplication modulo $x^\ell - 1$ we need only $O(\ell)$ arithmetic operations.

We show that the complexity of the proposed CRT-based QC matrix multiplication algorithm is $O(nm\ell \log \ell)$ arithmetic operations for the CRT domain calculations plus additional $O((n+m)\ell \log^2 \ell \log\log \ell)$ operations to transform the data into the CRT domain and back.

We also consider the problem of encoding for high-rate QC LDPC codes, where it is possible to utilize the sparseness of its QC parity-check matrix $\mathbf{H}$. In this case we can use a decomposition $\mathbf{H} = (\mathbf{H}_{\rm u}, \mathbf{H}_{\rm p})$, where the QC submatrices $\mathbf{H}_{\rm u}$ and $\mathbf{H}_{\rm p}$ correspond respectively to the information part $\mathbf{u}$ and the parity part $\mathbf{p}$ of the codeword. The encoding can be done [6] in two stages: (1) calculate $\mathbf{s} = -\mathbf{H}_{\rm u}\mathbf{u}$ and (2) find $\mathbf{p}$ as a solution to the equation $\mathbf{H}_{\rm p}\mathbf{p} = \mathbf{s}$. We propose to use a generalized inverse[3] $\mathbf{H}_{\rm p}^{+}$ of $\mathbf{H}_{\rm p}$ to find a solution $p = \mathbf{H}_{\rm p}^{+}\mathbf{s}$ in the second stage. Though every QC matrix $\mathbf{H}_{\rm p}$ has a generalized inverse there exist QC matrices that do not have QC generalized inverses[4]. Thus it is not always possible to use fast CRT-based QC matrix multiplication in the second stage. In this paper we give necessary and sufficient conditions when this QC generalized inverse exists and show how to find it. As a consequence, we show that it always exists if the circulant size ℓ is coprime to the characteristic of the field $\mathbb{F}_q$.

The remainder of the paper is organized as follows. In Section II we review some standard encoding algorithms for QC codes. In Section III we describe the CRT-based QC matrix multiplication algorithm and analyze its complexity. In Section IV we study generalized inverses for QC matrices. In the last section we give some final remarks and compare our algorithm with the one proposed recently in [12].

II. Encoding algorithms for QC codes

Usually a QC (N, K)-code over a finite field $\mathbb{F}_q$, where $N = n\ell$, is represented by an $m\ell \times n\ell$ block parity-check matrix

$$\mathbf{H} = \underbrace{\begin{bmatrix} \mathbf{H}_{1,1} & \dots & \mathbf{H}_{1,k} & \mathbf{H}_{1,k+1} & \dots & \mathbf{H}_{1,n} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{H}_{m,1} & \dots & \mathbf{H}_{m,k} & \mathbf{H}_{m,k+1} & \dots & \mathbf{H}_{m,n} \end{bmatrix}}_{\mathbf{H}_{\rm u}\text{ (information part)}} \underbrace{\qquad\qquad}_{\mathbf{H}_{\rm p}\text{ (parity part)}}, \quad (2)$$

where each block $\mathbf{H}_{ij}$ is an $\ell \times \ell$ circulant matrix over $\mathbb{F}_q$. We call a row (column) of circulant submatrices a *circulant row* (*column*). Let $m' \geq m$ be the minimal number of circulant columns such that the corresponding QC submatrix $\mathbf{H}_{\rm p}$ has the same rank as the matrix $\mathbf{H}$. In almost all applications m' is equal or close to the number of circulant rows m. Let $k = n - m'$ and suppose that we have already permuted the circulant columns of the matrix $\mathbf{H}$ such that the information vector $\mathbf{u}$ correspond to the first k circulant columns (submatrix $\mathbf{H}_{\rm u}$) and the parity vector $\mathbf{p}$ to the last m' circulant columns (submatrix $\mathbf{H}_{\rm p}$).

If $\operatorname{rank}\mathbf{H}_{\rm p} = N - K < m'\ell$ then some of the parity symbols from $\mathbf{p}$ could be used as information symbols. In this paper we suppose that the difference $m'\ell - \operatorname{rank}\mathbf{H}_{\rm p}$ is small enough that we can safely ignore these additional information symbols and use them as parity symbols.

Most practical systematic encoding algorithms for QC codes can be roughly divided into two main categories:

- Algorithms based on a QC generator matrix $\mathbf{G}$ of the code. Let us call them $\mathbf{G}$-*based*. Given a systematic QC generator matrix $\mathbf{G} = (\mathbf{I} \mid \mathbf{G}_{\rm p})$ (for an algorithm to obtain it from $\mathbf{H}$, see [6]) we calculate the parity vector
$$\mathbf{p} = \mathbf{G}_{\rm p}^{\rm T}\mathbf{u}, \quad (3)$$
where $\mathbf{G}_{\rm p}^{\rm T}$ is also a QC matrix.
- Algorithms based on the parity-check matrix $\mathbf{H}$ of the code. Let us call them $\mathbf{H}$-*based*. We use the decomposition (2) of the parity-check matrix $\mathbf{H}$ and write the parity-check equations in the following form:
$$\mathbf{H}_{\rm u}\mathbf{u} + \mathbf{H}_{\rm p}\mathbf{p} = \mathbf{0}.$$
Then we calculate the vector
$$\mathbf{s} = -\mathbf{H}_{\rm u}\mathbf{u} \quad (4)$$
and find the parity vector $\mathbf{p}$ as a solution[5] of the equation
$$\mathbf{H}_{\rm p}\mathbf{p} = \mathbf{s}. \quad (5)$$

As we can see from the description of $\mathbf{G}$-based encoding algorithms they use only one QC matrix multiplication. This makes their implementation very simple and regular. The main drawback of $\mathbf{G}$-based encoders for QC LDPC codes is that they usually can not utilize the sparseness of the parity-check matrix $\mathbf{H}$. At the same time $\mathbf{H}$-based encoders utilize the sparseness of $\mathbf{H}$ when they perform matrix multiplication (4). This is particularly important for high-rate QC LDPC codes, where the matrix $\mathbf{H}_{\rm p}$ is small compared to $\mathbf{H}_{\rm u}$. Unfortunately, the way that one usually finds a solution to equation (5) heavily depends on the type of the matrix $\mathbf{H}_{\rm p}$ and does not work equally well for all QC matrices.

There have been proposed many methods for solving equation (5) in an $\mathbf{H}$-based encoder for some specific classes of QC LDPC codes. When the matrix $\mathbf{H}_{\rm p}$ is invertible one general approach to solve equation (5) is to use the inverse $\mathbf{H}_{\rm p}^{-1}$ and obtain $\mathbf{p} = \mathbf{H}_{\rm p}^{-1}\mathbf{u}$. It can be proved [6] that if $\mathbf{H}_{\rm p}$ is a QC matrix then $\mathbf{H}_{\rm p}^{-1}$ is also a QC matrix. Thus the CRT-based QC matrix multiplication algorithm described in the next section can also be used to perform the multiplication $\mathbf{H}_{\rm p}^{-1}\mathbf{u}$. Unfortunately, there are many practical cases when the matrix $\mathbf{H}_{\rm p}$ is not invertible. For example, when the column weight of a column-regular QC LDPC code over $\mathbb{F}_2$ is even the matrix $\mathbf{H}_{\rm p}$ can never be invertible since the sum of all its rows is the all-zero vector. If $\mathbf{H}_{\rm p}$ is not invertible then it is possible to use a generalized inverse of the matrix $\mathbf{H}_{\rm p}$ instead of $\mathbf{H}_{\rm p}^{-1}$. A *generalized inverse* of an $m \times n$ matrix $\mathbf{A}$ is an $n \times m$ matrix $\mathbf{G}$ such that $\mathbf{AGA} = \mathbf{A}$. The matrix $\mathbf{G}$ may not exist and is not necessary unique. It can be used to obtain a solution $\mathbf{x}$ of the equation $\mathbf{Ax} = \mathbf{b}$ from the vector $\mathbf{b}$ when it is known that

[3] It is defined in the next section and coincides with the inverse $\mathbf{H}_{\rm p}^{-1}$ if $\mathbf{H}_{\rm p}$ is invertible.

[4] Of the same circulant size ℓ.

[5] It is not unique when $\mathbf{H}_{\rm p}$ is not invertible.

this equation has some solution[6] $\mathbf{x}_0$. Indeed, we can always set $\mathbf{x} = \mathbf{G}\mathbf{b}$ since

$$\mathbf{A}\mathbf{G}\mathbf{b} = \mathbf{A}\mathbf{G}\mathbf{A}\mathbf{x}_0 = \mathbf{A}\mathbf{x}_0 = \mathbf{b}.$$

Hence when the matrix $\mathbf{H}_{\mathrm{p}}$ has a generalized inverse $\mathbf{H}_{\mathrm{p}}^{+}$ we can find a solution to equation (5) as follows

$$\mathbf{p} = \mathbf{H}_{\mathrm{p}}^{+}\mathbf{u}. \tag{6}$$

In this paper we propose a new general approach to systematic encoding of QC codes based on the Chinese remainder theorem (CRT). It can either be used with $\mathbf{G}$-based or $\mathbf{H}$-based encoder. The main idea of this approach is to apply the fast CRT-based QC matrix multiplication algorithm introduced in the next section to the step (3) of the $\mathbf{G}$-based encoder and if $\mathbf{H}_{\mathrm{p}}$ has a QC generalized inverse to the steps (4) and (6) of the $\mathbf{H}$-based encoder. It should be mentioned that we do not need to apply the CRT-based algorithm to the step (4) for QC LDPC codes since $\mathbf{H}_{\mathrm{u}}$ is a sparse matrix. Hence the complexity of the proposed $\mathbf{G}$-based and $\mathbf{H}$-based encoders is defined by the complexity of the CRT-based algorithm analyzed in the next section.

III. CRT-based QC matrix multiplication

A. Polynomial Representation of QC Matrices

In this paper we adopt the polynomial representation of QC matrices used in [7], [8]. Let $\mathbb{F}$ be a field. Denote by $\mathbb{F}[x]$ the ring of polynomials over $\mathbb{F}$. For any polynomial $p(x) \in \mathbb{F}[x]$ of degree d we consider the ring $\mathbb{F}[x]/(p(x))$ of polynomials $f_0 + f_1 x + \cdots + f_{d-1}x^{d-1} \in \mathbb{F}[x]$ with addition and multiplication modulo $p(x)$. By $\mathbb{F}^d$ denote the d-dimensional space of the $d \times 1$ column vectors over $\mathbb{F}$. We identify an element $f(x) \in \mathbb{F}[x]/(p(x))$ with the corresponding column vector $\mathbf{f} = (f_0, \ldots, f_{d-1})^{\mathrm{T}} \in \mathbb{F}^d$.

By $\mathbb{F}^{\langle \ell \rangle}$ denote the ring $\mathbb{F}[x]/(x^\ell - 1)$. We use the standard identification of the circulant $\ell \times \ell$ matrices over $\mathbb{F}$ with the elements of the ring $\mathbb{F}^{\langle \ell \rangle}$, where a column vector $\mathbf{f} \in \mathbb{F}^{\langle \ell \rangle}$ corresponds to the circulant matrix with the first column equal to $\mathbf{f}$. Using this identification we can consider an $m\ell \times n\ell$ QC matrix over $\mathbb{F}$ of circulant size ℓ as an $m \times n$ matrix over the ring $\mathbb{F}^{\langle \ell \rangle}$. We also consider $n \times 1$ column vectors over $\mathbb{F}^{\langle \ell \rangle}$ as $n\ell \times 1$ column vectors over $\mathbb{F}$. Given the above identification we consider multiplication of an $m\ell \times n\ell$ QC matrix by an $n\ell \times 1$ column vector over $\mathbb{F}$ as multiplication of an $m \times n$ matrix by an $n \times 1$ column vector over $\mathbb{F}^{\langle \ell \rangle}$.

B. The Chinese Remainder Theorem

Here we briefly remind the Chinese Remainder Theorem (CRT) for the ring $\mathbb{F}[x]$ (see [9, Section 5.4] for a proof) and show how it can be used for fast QC matrix multiplication. We say that polynomials $p_1(x), \ldots, p_s(x)$ are *pairwise coprime* if we have $\gcd(p_i(x), p_j(x)) = 1$ for all $i \neq j$.

[6]This is always the case for equation (5).

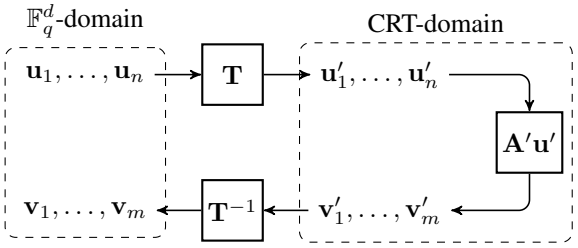

Fig. 1. CRT-based QC matrix multiplication

Theorem 1 (CRT)**.** *If $p_1(x), \ldots, p_s(x)$ are pairwise coprime polynomials from $\mathbb{F}[x]$ and $p(x) = p_1(x) \ldots p_s(x)$, then the ring $\mathbb{F}[x]/(p(x))$ is isomorphic to the direct product of rings*

$$\mathbb{F}[x]/(p_1(x)) \times \cdots \times \mathbb{F}[x]/(p_s(x))$$

with the following one-to-one correspondence between elements

$$f(x) \longleftrightarrow (f(x) \bmod p_1(x), \ldots, f(x) \bmod p_s(x)).$$

Let $d_i = \deg p_i(x)$, $i = \overline{1,s}$, and $d = \deg p(x) = d_1 + \cdots + d_s$. As we mentioned earlier we represent elements of $\mathbb{F}[x]/(p(x))$ as column vectors over $\mathbb{F}$. We refer to this representation as *the $\mathbb{F}^d$-domain*. From Theorem 1 it follows that each element $\mathbf{u} \in \mathbb{F}[x]/(p(x))$ can be uniquely represented as the column vector $(\mathbf{u}_1, \ldots, \mathbf{u}_s)^{\mathrm{T}} \in \mathbb{F}^d$, where $\mathbf{u}_i \in \mathbb{F}[x]/(p_i(x))$, $i = \overline{1,s}$. We refer to this representation as *the CRT domain*. It is readily seen that the transformation $\mathcal{T}$ from the $\mathbb{F}^d$-domain to the CRT domain is $\mathbb{F}$-linear. The same is also true for the inverse transformation $\mathcal{T}^{-1}$ from the CRT domain back to the $\mathbb{F}^d$-domain. By $\mathbf{T}$ and $\mathbf{T}^{-1}$ denote the $d \times d$ matrices over the field $\mathbb{F}$ for the linear operators $\mathcal{T}$ and $\mathcal{T}^{-1}$ respectively. It is not hard to see that the j-th column of the matrix $\mathbf{T}$ is the column vector $(\mathbf{t}_1, \ldots, \mathbf{t}_s)^{\mathrm{T}} \in \mathbb{F}^d$, where $t_i(x) = x^{j-1} \bmod p_i(x)$, $i = \overline{1,s}$, $j = \overline{1,d}$. The matrix $\mathbf{T}^{-1}$ is the matrix inverse of $\mathbf{T}$.

C. Algorithm Description

Let us fix a natural number ℓ and a finite field $\mathbb{F}_q$. Consider a matrix $\mathbf{A} = (a_{ij})_{m \times n}$ and a vector $\mathbf{u} = (\mathbf{u}_1, \ldots, \mathbf{u}_n)^{\mathrm{T}}$ over the ring $\mathbb{F}_q^{\langle \ell \rangle}$. We also choose[7] a polynomial $p(x) = p_1(x) \ldots p_s(x)$ of degree $d \geq \ell$, where $p_1(x)$, …, $p_s(x)$ are distinct irreducible polynomials over $\mathbb{F}_q$. In order to find the vector $\mathbf{v} = (\mathbf{v}_1, \ldots, \mathbf{v}_n)^{\mathrm{T}}$, where $\mathbf{v} = \mathbf{A}\mathbf{u}$, we use the CRT-domain for the polynomial $p(x)$. First consider the simpler case, where $d = \ell$ and ℓ is coprime to the characteristic of $\mathbb{F}_q$. In this case we can choose $p(x) = x^\ell - 1$ since the polynomial $p(x)$ is square-free[8] and it factors into irreducible polynomials over $\mathbb{F}_q$. We proceed with the following steps (see Fig. 1):

1) Convert the input vector $\mathbf{u} = (u_1, \ldots, u_n)^{\mathrm{T}}$ into the CRT-domain: $\mathbf{u}'_i = \mathcal{T}\mathbf{u}_i$, $i = \overline{1,n}$;

[7]We describe below how to choose it properly.

[8]This follows from $\gcd\left((x^\ell - 1)', x^\ell - 1\right) = \gcd\left(\ell x^{\ell-1}, x^\ell - 1\right) = 1$.

2) Compute $\mathbf{v}' = \mathbf{A}'\mathbf{u}'$ in the CRT domain using the standard matrix multiplication algorithm, where $\mathbf{A}'$ is the matrix $\mathbf{A}$ in the CRT domain and $\mathbf{u}' = (\mathbf{u}'_1, \ldots, \mathbf{u}'_n)^{\mathrm{T}}$;
3) Convert the vector $\mathbf{v} = (\mathbf{v}_1, \ldots, \mathbf{v}_m)^{\mathrm{T}}$ back into the $\mathbb{F}_q^d$-domain: $\mathbf{v}_i = \mathcal{T}^{-1}\mathbf{v}'_i$, $i = \overline{1,m}$.

Now consider the general case where ℓ is not necessary coprime to the characteristic of the field $\mathbb{F}_q$. We choose any square-free polynomial $p(x)$ such that $d = \deg p(x) \geq 2\ell - 1$. Since $\ell \leq d$ and hence $\mathbb{F}_q^{\langle \ell \rangle} \subseteq \mathbb{F}_q[x]/(p(x))$, we can identify the elements of $\mathbb{F}_q^{\langle \ell \rangle}$ with the column vectors from $\mathbb{F}_q^d$ that have zeros at the last $d - \ell$ positions. Thus we can proceed with all three steps described above and obtain the vector $\mathbf{v} = (\mathbf{v}_1, \ldots, \mathbf{v}_m)^{\mathrm{T}}$. Since $\mathbf{v}$ is in the $\mathbb{F}_q^d$-domain, we need to reduce each $\mathbf{v}_i$, $i = \overline{1,m}$, modulo $x^\ell - 1$ to obtain an element of $\mathbb{F}_q^{\langle \ell \rangle}$. This extra step requires only $O(m\ell)$ additions in the field $\mathbb{F}_q$ and has a negligible impact on the total algorithm complexity. The correctness of the above algorithm follows from the following fact. If we multiply $\mathbf{A}$ by $\mathbf{u}$ in the ring $\mathbb{F}_q[x]$ instead of $\mathbb{F}_q^{\langle \ell \rangle}$ and then reduce the result modulo $x^\ell - 1$, then the polynomials we obtain are exactly the same as if we would do all the calculations in $\mathbb{F}_q^{\langle \ell \rangle}$. On the other hand, it is clear that every polynomial involved in the above calculations in $\mathbb{F}[x]$ has a degree of no more than $2(\ell - 1)$. Thus we can use the ring $\mathbb{F}[x]/(p(x))$ instead of $\mathbb{F}[x]$ since $\deg p(x) = d > 2(\ell - 1)$ and it has enough "precision" to correctly perform the calculations.

D. Complexity Analysis

We estimate the complexity of the CRT-based algorithm in terms of arithmetic operations in $\mathbb{F}_q$. It is known [9, Section 10.3] that the transformations $\mathcal{T}$ and $\mathcal{T}^{-1}$ can be implemented using $O(\ell \log^2 \ell \log\log \ell)$ operations[9]. Thus the complexity of the steps 1 and 3 is $O((n+m)\ell \log^2 \ell \log\log \ell)$. For the field $\mathbb{F}_2$ the transformations $\mathcal{T}$ and $\mathcal{T}^{-1}$ can also be implemented as $\ell \times \ell$ binary matrix multiplication. This requires at most ℓ^2 two-input XOR gates when we implement it in hardware.

The complexity of the step 2 can be estimated as follows. First, it is not hard to show that there is a constant C such that multiplication in each ring $\mathbb{F}_q[x]/(p_i(x))$, $i = \overline{1,s}$, can be implemented using at most Cd_i^2 operations, where $d_i = \deg p_i(x)$. Thus the complexity of one multiplication in the CRT domain is at most $C\sum_{i=1}^s d_i^2$ operations. If we set $p(x) = x^{q^t - 1} - 1$, where $t = \lceil \log_q 2\ell \rceil$; then $2\ell - 1 \leq q^t - 1$ and since each irreducible factor $p_i(x)$ of $p(x)$ is the minimal polynomial of some element from the extension field $\mathbb{F}_{q^t}$, we see that $d_i = \deg p_i(x) \leq t$. Hence we obtain

$$C\sum_{i=1}^{s} d_i^2 \leq Ct\sum_{i=1}^{s} d_i = Ct(q^t - 1) = O(\ell \log \ell).$$

and the complexity of the step 2 is $O(nm\ell \log \ell)$ since it uses at most $2nm$ additions and multiplications in the CRT domain.

[9]To be more precise, it is equal to $O(\mathrm{M}(\ell)\log \ell)$, where $\mathrm{M}(\ell) = O(\ell \log \ell \log\log \ell)$ is the complexity of two degree ℓ polynomials multiplication.

The amount of memory required to store the matrix $\mathbf{A}'$ is the same as for the initial matrix $\mathbf{A}$ in the simple case, where ℓ is coprime to the characteristic of $\mathbb{F}_q$. However in the general case $\mathbf{A}'$ requires asymptotically two times more space than $\mathbf{A}$.

IV. Generalized inverses of QC matrices

A. Regular Matrices over Rings

Consider some $m \times n$ matrix $\mathbf{A}$ over a ring[10] R. An $n \times m$ matrix $\mathbf{G}$ is said to be a *generalized inverse* of $\mathbf{A}$ if $\mathbf{AGA} = \mathbf{A}$. We say that $\mathbf{A}$ is *regular* if it has a generalized inverse. Thus to give necessary and sufficient conditions when a QC matrix over a field $\mathbb{F}$ has a QC generalized inverse we need to describe all regular matrices over the ring $\mathbb{F}^{\langle \ell \rangle}$.

We also say that $a \in R$ is *regular* if there exists an element $g \in R$ such that $aga = a$. In that case we also call g a *generalized inverse* of the element a and denote[11] it by a^+. A ring R is called (von Neumann) *regular* if every element of R is regular. It is readily seen that any field is a regular ring and $x^+ = x^{-1}$ for $x \neq 0$ and $0^+ = 0$. It is also clear that a direct product of regular rings is regular.

In this section we review some simple facts about regular matrices over general rings (see [13], pp. 32–40). Let R be a ring. We say that two $m \times n$ matrices $\mathbf{A}$ and $\mathbf{A}'$ over R are *equivalent* if $\mathbf{A}' = \mathbf{UAV}$ for some invertible matrices $\mathbf{U}$ and $\mathbf{V}$. It is easy to see that this relation is reflexive, symmetric and transitive. Thus it is indeed an equivalence relation on the set of all $m \times n$ matrices over the ring R. Moreover, as the following lemma shows the property of a matrix to be regular is invariant under this equivalence relation.

Lemma 1. *For any two equivalent $m \times n$ matrices $\mathbf{A}$ and $\mathbf{A}'$ over a ring R such that $\mathbf{A}' = \mathbf{UAV}$ the following conditions hold:*

(i) *The matrix $\mathbf{A}$ is regular iff the matrix $\mathbf{A}'$ is regular.*
(ii) *If a matrix $\mathbf{G}$ is a generalized inverse of $\mathbf{A}$, then the matrix $\mathbf{G}' = \mathbf{V}^{-1}\mathbf{GU}^{-1}$ is a generalized inverse of $\mathbf{A}'$.*

In the general case, it is not easy to say whether a matrix $\mathbf{A} = (a_{ij})_{m\times n}$ over a ring R is regular, even if we know all the regular elements in R. However, when the matrix $\mathbf{A}$ is diagonal (i.e., $a_{ij} = 0$ whenever $i \neq j$) the following lemma gives a complete characterization of regular matrices in terms of regular elements in the ring R.

Lemma 2. *For any diagonal matrix $\mathbf{A} = (a_{ij})_{m\times n}$ over a ring R the following conditions hold:*

(i) *The matrix $\mathbf{A}$ is regular iff all its diagonal elements a_{ii} are regular in R.*
(ii) *If every diagonal element a_{ii} of the matrix $\mathbf{A}$ has a generalized inverse a_{ii}^+ in R, then the matrix $\mathbf{G} = (g_{ij})_{n\times m}$ is a generalized inverse of $\mathbf{A}$, where*

$$g_{ij} = \begin{cases} a_{ii}^+, & \text{if } i = j \\ 0, & \text{if } i \neq j \end{cases}. \tag{7}$$

[10]In this section, by a ring we mean a commutative ring with identity. Though most of the results are also valid for general rings.

[11]It is not necessary unique.

B. Regular Matrices over the Ring $\mathbb{F}^{\langle \ell \rangle}$

Here we describe all regular matrices over the ring $\mathbb{F}^{\langle \ell \rangle}$ in terms of regular elements of $\mathbb{F}^{\langle \ell \rangle}$. We first show that any $m \times n$ matrix $\mathbf{A}$ over the ring $\mathbb{F}^{\langle \ell \rangle}$ is equivalent to a diagonal matrix. Indeed, since the elements of $\mathbb{F}^{\langle \ell \rangle}$ are polynomials[12], we can regard $\mathbf{A}$ as a matrix with entries in the ring $\mathbb{F}[x]$. It is very well known (see [14], pp. 130–141) that any such matrix can be represented as

$$\mathbf{A} = \mathbf{UDV} \quad (\text{over } \mathbb{F}[x]), \tag{8}$$

where $\mathbf{D}$ is diagonal and $\mathbf{U}$, $\mathbf{V}$ are invertible matrices over the ring $\mathbb{F}[x]$. Under appropriate assumptions on the diagonal matrix $\mathbf{D}$, it is unique and called *the Smith normal form over* $\mathbb{F}[x]$ of the matrix $\mathbf{A}$. In equation (8) the matrices are over the ring $\mathbb{F}[x]$. Considering this equation modulo $x^\ell - 1$, we get

$$\mathbf{A} = \mathbf{U}'\mathbf{D}'\mathbf{V}' \quad (\text{over } \mathbb{F}^{\langle \ell \rangle}), \tag{9}$$

where $\mathbf{U}'$, $\mathbf{D}'$, and $\mathbf{V}'$ are correspondingly the matrices $\mathbf{U}$, $\mathbf{D}$, and $\mathbf{V}$ modulo $x^\ell - 1$. Since $\mathbf{U}$ and $\mathbf{V}$ are invertible matrices over $\mathbb{F}[x]$, it follows that their determinants are non-zero constant polynomials. Hence these determinants are invertible modulo $x^\ell - 1$ and the matrices $\mathbf{U}'$ and $\mathbf{V}'$ are invertible over the ring $\mathbb{F}^{\langle \ell \rangle}$. Therefore we proved that the matrix $\mathbf{A}$ is equivalent (over $\mathbb{F}^{\langle \ell \rangle}$) to the diagonal matrix $\mathbf{D}'$, which we call *the Smith normal form over* $\mathbb{F}^{\langle \ell \rangle}$ of $\mathbf{A}$. This fact, combined with Lemmas 1 and 2, gives us the following result.

Theorem 2. *An $m \times n$ matrix over the ring $\mathbb{F}^{\langle \ell \rangle}$ is regular iff all the diagonal elements in its Smith normal form over $\mathbb{F}^{\langle \ell \rangle}$ are regular in $\mathbb{F}^{\langle \ell \rangle}$.*

C. Regular Elements of the Ring $\mathbb{F}^{\langle \ell \rangle}$

From Theorem 2 it follows that to give a complete characterization of regular matrices over the ring $\mathbb{F}^{\langle \ell \rangle}$ we need to describe all regular elements in $\mathbb{F}^{\langle \ell \rangle}$. Moreover combined with Lemmas 1 and 2 it gives us a way to find a generalized inverse of a regular matrix over $\mathbb{F}^{\langle \ell \rangle}$. It is known [15] that if the characteristic p of the field $\mathbb{F}$ is zero or coprime to ℓ the ring $\mathbb{F}^{\langle \ell \rangle}$ is isomorphic to a direct product of fields. Hence $\mathbb{F}^{\langle \ell \rangle}$ is regular[13] and any matrix over it is regular. If $\ell = p^e \ell'$, where $p \nmid \ell'$ and $e > 0$, the ring $\mathbb{F}^{\langle \ell \rangle}$ is isomorphic [15] to the direct product $R_1 \times \cdots \times R_s$ of the rings $R_i = \mathbb{F}[x]/\big(f_i(x)\big)^{p^e}$, $i = \overline{1,s}$. It is easy to see that an element a of this product is regular iff each its component a_i is regular in R_i, $i = \overline{1,s}$. If $a = (a_1, \ldots, a_s)$ is regular we can use $a^+ = (a_1^+, \ldots, a_s^+)$ as its generalized inverse, where a_i^+ is a generalized inverse of a_i, $i = \overline{1,s}$. Hence to finish the classification of regular elements in $\mathbb{F}^{\langle \ell \rangle}$ we need to describe regular elements of the rings $R_1, \ldots, R_s$. It turns out that the only regular elements in a ring of this type are its zero and its units[14].

[12] We assume in this paper that the elements of $\mathbb{F}^{\langle \ell \rangle} = \mathbb{F}[x]/(x^\ell - 1)$ are polynomials $a_0 + a_1 x + \cdots + a_{\ell-1} x^{\ell-1}$.

[13] As a direct product of regular rings.

[14] A *unit* or an *invertible element* of a ring R is an element $u \in R$ such that it has the multiplicative inverse $u^{-1} \in R$, i.e., $uu^{-1} = u^{-1}u = 1$.

Lemma 3. *Let $R = \mathbb{F}[x]/\big(f(x)\big)^n$, where $f(x)$ is an irreducible polynomial over the field $\mathbb{F}$. Then a polynomial $a(x)$ is regular in R iff it is either 0 or coprime to $f(x)$.*

V. Conclusion and Related Work

We have shown that a systematic encoding can be implemented with much less complexity using the CRT-based QC matrix multiplication algorithm. In [12] the ETD encoder was proposed, which has a similar complexity. It uses the Fourier transform domain instead of the CRT domain to speed-up the computations. Unfortunately, it is not systematic. Moreover, it has a high complexity for some particular circulant sizes ℓ (e.g., $\ell = 2^s$ and the field $\mathbb{F}_2$). At the same time the CRT-based encoder is systematic and has a low complexity independently of the circulant size. However it is more efficient and requires less memory when the circulant size ℓ is coprime with the field characteristic. In the latter case it is also possible to use the $\mathbf{H}$-based encoder since every QC matrix has a QC generalized inverse.

References

[1] R. Townsend and E. Weldon, Jr., "Self-orthogonal quasi-cyclic codes," *Information Theory, IEEE Transactions on*, vol. 13, no. 2, pp. 183–195, 1967.

[2] T. Kasami, "A Gilbert-Varshamov bound for quasi-cycle codes of rate 1/2 (corresp.)," *Information Theory, IEEE Transactions on*, vol. 20, no. 5, p. 679, 1974.

[3] C. Martinez-Perez and W. Willems, "Is the class of cyclic codes asymptotically good?" *Information Theory, IEEE Transactions on*, vol. 52, no. 2, pp. 696–700, 2006.

[4] R. G. Gallager, *Low-Density Parity-Check Codes*. M.I.T. Press, Cambridge, MA, 1963.

[5] M. P. C. Fossorier, "Quasicyclic low-density parity-check codes from circulant permutation matrices," *Information Theory, IEEE Transactions on*, vol. 50, no. 8, pp. 1788–1793, 2004.

[6] Z. Li, L. Chen, L. Zeng, S. Lin, and W. H. Fong, "Efficient encoding of quasi-cyclic low-density parity-check codes," *Communications, IEEE Transactions on*, vol. 54, no. 1, pp. 71–81, 2006.

[7] K. Lally and P. Fitzpatrick, "Algebraic structure of quasicyclic codes," *Discrete Applied Mathematics*, vol. 111, no. 1–2, pp. 157–175, 2001.

[8] R. Smarandache and P. Vontobel, "Quasi-cyclic LDPC codes: Influence of proto- and tanner-graph structure on minimum Hamming distance upper bounds," *IEEE Transactions on Information Theory*, vol. 58, no. 2, pp. 585–607, 2012.

[9] J. von zur Gathen and J. Gerhard, *Modern Computer Algebra*. Cambridge University Press, 2003.

[10] M. Baldi, M. Bodrato, and F. Chiaraluce, "A new analysis of the McEliece cryptosystem based on QC-LDPC codes," in *Security and Cryptography for Networks*, ser. LNCS. Springer Berlin Heidelberg, 2008, vol. 5229, pp. 246–262.

[11] S. Winograd, *Arithmetic Complexity of Computations*, ser. CBMS-NSF Regional Conference Series in Applied Mathematics. Society for Industrial and Applied Mathematics, 1980.

[12] Q. Huang, L. Tang, S. He, Z. Xiong, and Z. Wang, "Low-complexity encoding of quasi-cyclic codes based on Galois Fourier transform," *Communications, IEEE Transactions on*, vol. 62, no. 6, pp. 1757–1767, June 2014.

[13] K. P. S. Bhaskara Rao, *Theory of Generalized Inverses Over Commutative Rings*, ser. Algebra, Logic and Applications. London and New York: CRC Press, 2002, vol. 17.

[14] F. R. Gantmacher, *The Theory of Matrices, Vol. 1*, 2nd ed., ser. Chelsea Publishing Series. AMS Chelsea Pub., 1990.

[15] S. Ling, H. Niederreiter, and P. Solé, "On the algebraic structure of quasi-cyclic codes IV: Repeated roots," *Designs, Codes and Cryptography*, vol. 38, pp. 337–361, 2006.

Appendix A
Algebraic structure of the ring $\mathbb{F}^{\langle \ell \rangle}$

Let $\mathbb{F}$ be a field of characteristic p. The algebraic structure of the ring $\mathbb{F}^{\langle \ell \rangle}$ is well studied in the coding literature (see, e.g., [15]). Here we briefly review it in a slightly more general form when the field $\mathbb{F}$ is not required to be finite.

First, let us consider the special case when $p \nmid \ell$, i.e., the characteristic p of the field $\mathbb{F}$ is either zero or coprime to ℓ. In this case the polynomial $x^\ell - 1$ factors into a product of irreducible polynomials over $\mathbb{F}$

$$x^\ell - 1 = f_1(x) \cdots f_s(x). \tag{10}$$

This is true, since

$$\gcd\big((x^\ell - 1)', x^\ell - 1\big) = \gcd\big(\ell x^{\ell-1}, x^\ell - 1\big) = 1,$$

and the polynomial $x^\ell - 1$ is square-free.

In the general case we have[15] $\ell = p^e \ell'$, where $p \nmid \ell'$. Hence it follows that

$$x^\ell - 1 = x^{p^e \ell'} - 1 = (x^{\ell'} - 1)^{p^e}.$$

Moreover, since $p \nmid \ell'$, we can apply the factorization (10) to the polynomial $x^{\ell'} - 1$ and obtain that

$$x^\ell - 1 = \big(f_1(x)\big)^{p^e} \cdots \big(f_s(x)\big)^{p^e}. \tag{11}$$

Since the polynomials $\big(f_1(x)\big)^{p^e}, \ldots, \big(f_s(x)\big)^{p^e}$ are pairwise coprime, from the Chinese remainder theorem it follows that the ring $\mathbb{F}^{\langle \ell \rangle}$ is isomorphic to the direct product

$$R_1 \times \cdots \times R_s \tag{12}$$

of the rings $R_i = \mathbb{F}[x]/\big(f_i(x)\big)^{p^e}$, $i = \overline{1, s}$.

In the case $p \nmid \ell$ we have $e = 0$ and the rings $R_1, \ldots, R_s$ are in fact fields, since the polynomials $f_1(x), \ldots, f_s(x)$ are irreducible over $\mathbb{F}$.

Appendix B
Proof of Lemma 1

Proof: Since the equivalence relation on matrices is symmetric, it is clear that (ii) implies (i). The proof of (ii) follows from the direct calculation:

$$\mathbf{A}'\mathbf{G}'\mathbf{A}' = \mathbf{U}\mathbf{A}\mathbf{V}\mathbf{V}^{-1}\mathbf{G}\mathbf{U}^{-1}\mathbf{U}\mathbf{A}\mathbf{V} = \mathbf{U}\mathbf{A}\mathbf{V} = \mathbf{A}',$$

where we use the fact that $\mathbf{AGA} = \mathbf{A}$. ∎

Appendix C
Proof of Lemma 2

Proof: Let $\mathbf{A} = (a_{ij})_{m \times n}$ be a diagonal matrix over a ring R. For any matrix $\mathbf{G} = (g_{ij})_{n \times m}$ over R the equation $\mathbf{AGA} = \mathbf{A}$ can be written as

$$a_{ij} = \sum_{\substack{1 \le p \le n \\ 1 \le q \le m}} a_{ip} g_{pq} a_{qj}.$$

[15]We assume here that $0^0 = 1$ in order to include the case $p = 0$ and $e = 0$.

It is convenient to assume here that $a_{ij} = 0$ and $g_{pq} = 0$ whenever some of the indexes i, j, p, or q are out of the range. This assumption enables us to rewrite the previous equation in the form

$$a_{ij} = \sum_{p,q} a_{ip} g_{pq} a_{qj}, \tag{13}$$

where the sum is over all pairs of natural numbers. Since the matrix $\mathbf{A}$ is diagonal, it follows that a term $a_{ip} g_{pq} a_{qj}$ in the last sum can be non-zero only if $p = i$ and $q = j$. Thus we can simplify equation (13) as follows

$$a_{ij} = a_{ii} g_{ij} a_{jj}. \tag{14}$$

Suppose now that the matrix $\mathbf{A}$ is regular and there exists a matrix $\mathbf{G}$ such that $\mathbf{AGA} = \mathbf{A}$; then from equation (14) we have $a_{ii} = a_{ii} g_{ii} a_{ii}$ for all i and hence all the diagonal elements a_{ii} of $\mathbf{A}$ are regular in the ring R.

On the other hand, if every diagonal element a_{ii} of the matrix $\mathbf{A}$ is regular and has a generalized inverse a_{ii}^+ in R, then it is easy to see that the matrix $\mathbf{G}$ defined by equation (7) satisfies equation (14). Hence we have $\mathbf{AGA} = \mathbf{A}$ and G is a generalized inverse of $\mathbf{A}$. ∎

Appendix D
Proof of Lemma 3

The proof is obvious when $n = 1$ since R is a field in this case. Thus assume that $n > 1$. It is known [9, Section 4.2] that the units of the ring R are precisely the elements coprime to $\big(f(x)\big)^n$ and hence to $f(x)$. Let us denote this set by $U(R)$. Clearly, the elements from $U(R) \cup \{0\}$ are regular in any ring. Therefore we need only prove that there are no other regular elements in the ring R. Assume the converse. Then there exists a regular $a(x) \in R$ such that $a(x) \notin U(R) \cup \{0\}$. Let $g(x)$ be its generalized inverse. Then we have $a(x)g(x)a(x) \equiv a(x) \bmod \big(f(x)\big)^n$. We can rewrite this as follows

$$\big(a(x)\big)^2 g(x) + q(x)\big(f(x)\big)^n = a(x), \tag{15}$$

where $q(x) \in \mathbb{F}[x]$. Since $a(x) \notin U(R) \cup \{0\}$, we have $a(x) = \big(f(x)\big)^s b(x)$, where $0 < s < n$ and $f(x) \nmid b(x)$. If we replace $a(x)$ by $\big(f(x)\big)^s b(x)$ in (15) and divide both sides by $\big(f(x)\big)^s$, we obtain

$$\big(f(x)\big)^s \big(b(x)\big)^2 g(x) + q(x)\big(f(x)\big)^{n-s} = b(x).$$

Since $n - s > 0$, we have that $f(x) \mid b(x)$. This contradiction proves the lemma.