Simplifying Quantum Circuits using Classical Bit-Serial Multipliers

Alejandro Ortega

1 Introduction

Unitary designs are finite ensembles of unitary matrices that approximate the Haar distribution over the complex unitary group. As quantum algorithms and protocols increasingly require generating random processes over the unitary group, the Haar measure provides a natural randomization measure that simplifies analysis of such protocols. However, sampling the Haar measure is infeasible, hence the interest in finite unitary designs that approximate the measure. The unitary designs derived from the Kerdock Set are of interest in quantum benchmarking to support improvements to fidelity, and in wireless communication to develop algorithms that support multi-user detection for massive random access and neighbor discovery [7].

The unitary design associated with the Kerdock set is a representation of the projective linear group, and it was first constructed in [2] by different methods. The connection to Kerdock codes simplifies the description of this design. There are three types of generator, and the type associated with multiplication by field elements, is the most challenging to implement efficiently. In this paper we approach implementation by making a connection to classical bit-serial multiplication, and we use the connection to reduce the gate complexity of the unitary design.

1.1 Foundations of Quantum Mechanics

The mathematical basis for fault-tolerant quantum computation consists of a group-theoretic framework centered on the Heisenberg-Weyl Group. Throughout, let $N = 2^m$ and denote the binary field by $\mathbb{F}_2$. The Heisenberg-Weyl Group HW_N arises in physics as the Pauli Group, where it describes the possible state transitions in an m-qubit quantum system, and as the extraspecial group in mathematics, where it is the foundation of orthogonal and symplectic geometry.

A single qubit is a 2-dimensional Hilbert space, where

$$e_0 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \qquad e_1 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

form a computational basis. A quantum state ψ is a superposition of e_0 and e_1 such that $\psi = \alpha e_0 + \beta e_1$ for $\alpha, \beta \in \mathbb{C}$ satisfying the $|\alpha|^2 + |\beta|^2 = 1$. This condition on α and β is known as the Born Rule.

Let $i \equiv \sqrt{-1}$. The Pauli matrices are

$$I_2, \quad X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad Y \equiv iXZ = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

where I_2 is the 2×2 identity matrix. An arbitrary quantum state can be written as linear combination of Pauli matrices and the basis state e_0

$$\psi = (\alpha_0 I_2 + \alpha_1 X + i\alpha_2 Z + \alpha_3 Y)e_0$$

1.2 The Heisenberg-Weyl and Clifford Groups

The Heisenberg-Weyl Group is constructed as m-fold Kronecker products of the computational basis elements scaled by powers of i [1]. Let $\otimes$ denote the usual Kronecker product. Suppose $a = (a_{m-1}, \ldots, a_1), b = (b_{m-1}, \ldots, b_1)$ are binary vectors in $\mathbb{F}_2^m$. Define the following operator as an m-fold Kronecker product

$$D(a, b) \equiv X^{a_{m-1}} Z^{b_{m-1}} \otimes \cdots \otimes X^{a_1} Z^{a_1}$$

The Heisenberg-Weyl Group HW_N consists of all scalar multiples of m-qubit Pauli matrices of the form $\omega D(a, b)$ for all $a, b \in \mathbb{F}_2^m$, where $\omega = i^c$ for $c = 1, 2, 3, 4$. The cardinality of HW_N is $4N^2$.

The standard symplectic inner product [8] for $\mathbb{F}_2^{2m}$ is given by

$$\langle [a, b], [a', b'] \rangle_{\mathrm{S}} \equiv a'b^T + b'a^T = [a, b]\Omega[a', b']^T$$

Where the symplectic form

$$\Omega = \begin{bmatrix} 0 & I_m \\ I_m & 0 \end{bmatrix}$$

In general, a $2m \times 2m$ matrix M with entries in $\mathbb{F}_2$ that satisfies $M\Omega M^T = \Omega$ is said to be a binary symplectic matrix.

Heisenberg-Weyl is a group with respect to matrix multiplication, where multiplication of the operator $D(a, b)$ satisfies

$$D(a, b)D(a', b') = (-1)^{a'b^T + b'a^T} D(a', b')D(a, b)$$

Hence, elements of the Heisenberg-Weyl group either commute or anti-commute, and commute if only if their symplectic inner product $\langle [a, b], [a', b'] \rangle_{\mathrm{S}} = 0$.

There exists an homomorphism $\phi : HW_N \to \mathbb{F}_2^{2m}$ defined by

$$\phi(\omega D(a,b)) \equiv [a,b] \ \forall \ \omega \in \mathbb{Z}_4^i$$

which allows elements of HW_N to be readily represented as binary vectors in $\mathbb{F}_2^{2m}$, up to scalar multiplication. The kernel of this homomorphism is $\langle \omega I_N \rangle$.

The Clifford Group Cliff_N is the normalizer of HW_N within the usual complex unitary group $\mathbb{U}_N$, and thus consists of all unitary matrices $g \in \mathbb{U}_N$ satisfying

$$\{g \mid gD(a,b)g^\dagger \in HW_N \text{ for all } D(a,b) \in HW_N\}$$

where $g^\dagger$ is the Hermitian transpose of g.

The Clifford Group is of interest because elements of Cliff_N are physical operators that act on quantum states, and thus correspond to quantum circuits. Clifford operators can be represented with $2m \times 2m$ binary symplectic matrices, providing an exponential reduction in size [8]. These symplectic matrices act as a binary control plane for the quantum computer. The group of symplectic $2m \times 2m$ binary matrices is called the symplectic group over $\mathbb{F}_2^{2m}$ and is denoted by $\text{Sp}(2m, \mathbb{F}_2)$.

The elements of Cliff_N are unitary automorphisms because they induce automorphisms of HW_N by conjugation. These inner automorphisms in HW_N preserve every conjugacy class $\{\pm D(a,b)\}$ and $\{\pm iD(a,b)\}$.

1.3 Unitary Designs

Generating random processes over the unitary group $\mathbb{U}_N$ has become increasingly prevalent in algorithms and protocols, where the Haar measure provides a natural randomization measure. However, sampling the Haar measure is infeasible since the number of gates grows exponentially with the number of qubits, hence the interest in unitary k-designs. A unitary k-design is a finite ensemble of unitary matrices that approximates the Haar distribution.

Unitary designs are described in [3]; let k be a positive integer. An ensemble is the set $\mathcal{E} = \{p_i, U_i\}_{i=1}^n$, where p_i is the probability of selecting a unitary matrix U_i. $\mathcal{E}$ is a unitary k-design if for all linear operators $X \in (\mathbb{C}^{\mathbb{N}})^{\otimes k}$,

$$\sum_{(p,U)\in\mathcal{E}} pU^{\otimes k} X (U^\dagger)^{\otimes k} = \int_{\mathbb{U}_N} d\eta(U) U^{\otimes k} X (U^\dagger)^{\otimes k}$$

where $\eta(\cdot)$ denotes the Haar measure on the unitary group $\mathbb{U}_N$. The linear transformations on each side are called k-fold twirls [11]. A unitary k-deisgn is defined by the property that an ensemble twirl coincides with the full unitary twirl.

The matrix $E(a,b)$ is defined as

$$E(a,b) \equiv i^{ab^T} D(a,b)$$

$E(a,b)$ is Hermitian since the matrices $D(a,b)$ are symmetric when $ab^T = 0$ and anti-symmetric when $ab^T = 1$. $E(a,b)$ satisfies $E(a,b)^2 = I_N$.

The automorphism induced by a Clifford element g satisfies

$$gE(a,b)g^\dagger = \pm E([a,b]F_g)$$

where

$$F_g = \begin{bmatrix} A_g & B_g \\ C_g & D_g \end{bmatrix} \in \mathrm{Sp}(2m, \mathbb{F}_2)$$

Thus, the the symplectic property of F_g is a consequence of the automorphism induced by g respecting commutativity in HW_N .

The graph Γ_N is defined on vertices $\pm E(a,b)$ for all $[a,b] \neq 0$. An edge connects two vertices $\pm E(a,b)$ and $\pm E(a',b')$ if the corresponding Pauli matrices commute. To simplify notation, the matrix $\pm E(a,b)$ is identified by $[a,b]$.

A strongly regular graph is defined in [6], and has parameters (n,t,λ,μ). This graph has n vertices each of degree t. The number of vertices joined to a pair of distinct vertices x,y is either λ or μ, depending on whether x,y are joined or not, respectively.

The graph Γ_N is strongly regular with parameters

$$n = N-1, t = \frac{N^2}{2} - 2, \lambda = \frac{N^2}{4} - 3, \mu = \frac{N^2}{4} - 1$$

The Clifford Group acts transitively on vertices, edges and non-edges of Γ_N, which is a well-known result in symplectic geometry.

Let $\mathcal{E} = \{p_i, U_i\}_{i=1}^n$ be an ensemble of Clifford elements. The ensemble is Pauli mixing if the induced distribution $(p_i, U_i E(a,b) U_i^\dagger)$ is uniform over all Hermitian Paulis [12]. The ensemble is Pauli 2-mixing if for every pair of distinct vertices

$$([a,b],[a',b'])$$

that are joined (resp. non-joined), then the distribution over

$$(U_i E(a,b) U_i^\dagger, U_i E(a',b') U_i^\dagger)$$

is uniform over all edges(resp. non-edges).

An ensemble $\mathcal{E}$ constructed such that the uniform distribution is imposed on a subgroup of Cliff_N is Pauli mixing if the group action is transitive on the vertices of Γ_N, and is Pauli 2-mixing if the group action is transitive on non-edges and edges. A well known result in the literature is that a Clifford ensemble that is Pauli mixing satisfies the criteria for a unitary 2-design [12]. Since Clifford is shown to act transitively on edges and non-edges of Γ_N, the Clifford Group forms a unitary 3-design.

1.4 The Kerdock Codes

The Kerdock codes are non-linear binary codes, where the exponentiated codewords are the eigenvectors of maximal commutative subgroups of HW_N [10]. We will provide the framework for the construction of the Kerdock Set. The finite field $\mathbb{F}_{2^m}$ is constructed from the binary field $\mathbb{F}_2$ by adjoining the root α of an irreducible polynomial $p(x)$ of degree m. The field $\mathbb{F}_{2^m}$ consists of polynomials in α of degree at most $m-1$.

The *trace map* Tr: $\mathbb{F}_{2^m} \to \mathbb{F}_2$ is defined by

$$\mathrm{Tr}(x) = x + x^2 + x^{2^2} + \ldots + x^{2^{m-1}}$$

The trace inner product $\langle xy \rangle_{\mathrm{Tr}}$ is a symmetric bilinear form, and thus there exists a binary symmetric matrix A for which $\mathrm{Tr}(xy) = xAy^T$. This $m \times m$ matrix A is defined over the primal basis, which consist of powers of α:

$$A_{ij} = \mathrm{Tr}(\alpha^i \alpha^j) \quad i,j \in \{0,1,\ldots,m-1\}$$

Observe that this matrix A is a Hankel matrix, since if $i+j = h+k$ then $\mathrm{Tr}(\alpha^i\alpha^j) = \mathrm{Tr}(\alpha^h\alpha^k)$.

Let the primitive irreducible polynomial be given by

$$p(x) = p_0 + p_1 x + p_2 x^2 + \ldots + p_{m-1}x^{m-1} + x^m$$

Define the matrix $\mathcal{P}$ by

$$\mathcal{P} = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ & \vdots & & \ddots & 0 \\ 0 & 0 & 0 & \cdots & 1 \\ p_0 & p_1 & p_2 & \cdots & p_{m-1} \end{bmatrix}$$

which represents multiplication by the primitive element α. Then multiplication by $z \in \mathbb{F}_{2^m}$ can be written as the linear transformation $xz = x\mathcal{P}_z$, where $\mathcal{P}_z = \mathcal{P}^i$ for exactly the $i \in 0,1,\ldots,2^m-2$ that satisfies $z = \alpha^i$

For $0 \le r \le (m-1)/2$ and for $z = (z_0, z_1, \ldots, z_r)$ the bilinear form $\mathrm{Tr}(zxy)$ is represented by the binary symmetric matrix

$$P_z = \mathcal{P}_{z_0} A$$

Then the Kerdock Set $P_K(m)$ consists of all such matrices P_Z. Matrices in the Kerdock Set are non-singular.

It was shown in [10] that the the symmetry group of the union of mutually unbiased bases of the Kerdock codes form a unitary 2-design, providing the motivation for converting the Kerdock set into quantum gates.

The implementation of the design as a quantum circuit described in [2] had a quantum gate cost of $O(n \log n \log \log n)$, where $\mathcal{P}$ was the most challenging element of the design. Hence, we will show that classical bit-serial multipliers can be converted into efficient quantum circuits that perform $\mathcal{P}$, multiplication by a primitive element.

2 General Form Multiplication by a Primitive Element

Classical bit-serial circuits can efficiently perform multiplication in the finite field $\mathbb{F}_{2^m}$ by constructing a special pair of dual bases with respect to the trace inner product. We will follow the classical description of bit-serial multipliers described in [4] and translate them into the quantum world.

Let $\{\alpha_0, \alpha_1, \ldots, \alpha_{m-1}\}$ be a basis for $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$, known as the primal basis. The corresponding dual basis is defined to be the unique set of elements $\{\beta_0, \beta_1, \ldots, \beta_{m-1}\}$ such that

$$\mathrm{Tr}(\alpha_i \beta_j) = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$$

Although any independent set of m elements from $\mathbb{F}_{2^m}$ will suffice, only the primal basis of the form $\{1, \alpha, \ldots, \alpha^{m-1}\}$ will be considered. The matrix A can be interpreted as a conversion matrix from the primal to dual basis for $\mathbb{F}_{2^m}$.

The dual basis can be constructed from the primal basis through the following mechanical procedure. Since the trace inner product is non-degenerate, the matrix A is non-singular. Let $B = A^{-1}$. Then the elements of the dual basis is given by

$$\beta_j = \sum_{k=0}^{m-1} B_{kj} \alpha_k \qquad \text{for } j = 0, \ldots, m-1$$

The matrix B can similarly be interpreted as a conversion matrix from the dual basis to the primal basis.

Suppose $x \in \mathbb{F}_{2^m}$ and let the primal basis expansion of x be denoted by

$$x = \sum_{i=0}^{m-1} x_i \alpha_i \qquad x_i \in \{0, 1\}$$

Similarly, let the dual basis expansion of x be denoted by

$$x = \sum_{i=0}^{m-1} x'_i \beta_i \qquad x'_i \in \{0, 1\}$$

By defining the binary row vectors $\mathbf{x}$ and $\mathbf{x}'$ by

$$\mathbf{x} = [x_0, x_1, \ldots, x_{m-1}]$$
$$\mathbf{x}' = [x'_0, x'_1, \ldots, x'_{m-1}]$$

It can be easily verified that

$$\mathbf{x}' = \mathbf{x}A, \qquad x'_j = \mathrm{Tr}(x\alpha_j)$$
$$\mathbf{x} = \mathbf{x}'B, \qquad x_i = \mathrm{Tr}(x'\beta_i)$$

Henceforth, all $x \in \mathbb{F}_{2^m}$ will be identified by the binary row vector $\mathbf{x}$ of their primal basis expansion (or the binary row vector $\mathbf{x}'$ of their dual basis expansion, where appropriate). The benefits of the basis change lie in the ease of multiplying by primitive elements in the dual coordinate system.

Consider the dual basis expansion

$$x = x'_{m-1}\beta_{m-1} + x'_{m-2}\beta_{m-2} + \ldots + x'_0\beta_0$$

Since $x'_j = \mathrm{Tr}(x\alpha^j)$ for $j = 0, 1, \ldots, m-1$, it follows that multiplying x by α gives the relationship

$$(\alpha x)'_j = \mathrm{Tr}(\alpha x \cdot \alpha^j) = \mathrm{Tr}(x \cdot \alpha^{j+1})$$

Hence, multiplying by alpha in the dual coordinate system gives the following relation

$$\begin{cases} (\alpha x)'_j = x'_{j+1} & \text{for } j = 0, 1, \ldots, m-2 \\ (\alpha x)'_{m-1} = \mathrm{Tr}(x \cdot \alpha^m) \end{cases}$$

Thus, in the dual coordinate system multiplication by a primitive element corresponds to a simple shift register from classical computing. This shift register can be thought of as a permutation matrix that satisfies the shifting of the bits, and a parity tree operation that computes $(\alpha x)'_{m-1} = \mathrm{Tr}(x \cdot \alpha^m)$. In the quantum picture, this parity tree is a triangular CNOT gate that can be readily implemented.

Let $x \in \mathbb{F}_{2^m}$ be given in primal coordinates. Then the complete picture for multiplication by a primitive element consists of

1. Converting x to dual coordinates
2. Performing the bit-serial multiplication
3. Converting from dual to primal coordinates

2.1 Example for $\mathbb{F}_8$

Consider $m = 3$ and the corresponding finite field $\mathbb{F}_8$ constructed with the root α of the irreducible polynomial $p(x) = x^3 + x + 1$. Then the basis is

$$\{1, \alpha, \alpha^2\}$$

where α is a primitive root satisfying $\alpha^3 = \alpha + 1$. Let $x \in \mathbb{F}_8$ be represented by the binary vector $[x_0, x_1, x_2]$. Then the elements of $\mathbb{F}_8$ satisfy $\mathrm{Tr}(x) = x_0$. Hence, the matrix A is given by

$$A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} = \mathrm{Tr} \begin{bmatrix} \alpha^0 & \alpha^1 & \alpha^2 \\ \alpha^1 & \alpha^2 & \alpha^3 \\ \alpha^2 & \alpha^3 & \alpha^4 \end{bmatrix}$$

Observe that A is a permutation matrix and that $A^{-1} = A^T$. Thus,

$$B = A^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

and the corresponding dual basis is given by $\{1, \alpha^2, \alpha\}$. Thus, $x' = x \cdot A$ implies

$$\begin{aligned} x'_0 &= x_0 \\ x'_1 &= x_2 \\ x'_2 &= x_1 \end{aligned}$$

Recall that the bit-serial multiplier consists of a shift and parity tree operation in the dual coordinate system. The shift operation corresponds to the permutation $\pi_{(231.)}$. For $m = 3$, the parity tree corresponds to $\mathrm{Tr}(x'\alpha^3)$. Hence,

$$\begin{aligned} \mathrm{Tr}(x\alpha^3) &= x'_1 + x'_0 \\ &= x_2 + x_0 \end{aligned}$$

using duality relationships. Thus, the bit-serial multiplier is a transformation from $x' \rightarrow x'BSM$, where BSM is given by

$$\begin{aligned} BSM &= \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \end{aligned}$$

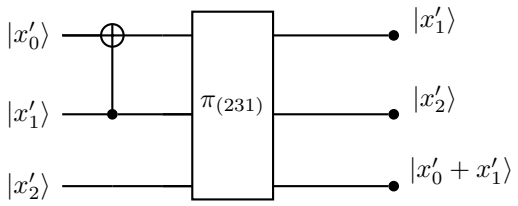

Figure 1: Quantum bit-serial circuit that performs multiplication by the primitive element satisfying $\alpha^3 = \alpha + 1$. Computed in the dual coordinate system.

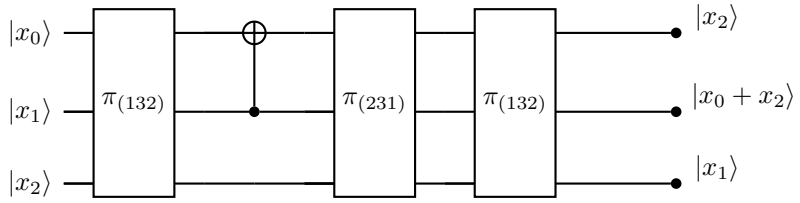

Figure 2: The complete quantum circuit diagram for multiplication by α, where α satisfies $\alpha^3 = \alpha + 1$.

where the latter equality corresponds to the permutation matrix $\pi_{(231)}$ and a lower triangular matrix that performs the parity tree as a CNOT operation. Thus, given an $x \in \mathbb{F}_8$ in dual coordinates, the above matrices perform multiplication by α in dual coordinates. The quantum circuit diagram of the bit-serial multiplier is given in Figure 1.

Let $x \in \mathbb{F}_8$ be given in primal coordinates. Recall that $A = A^{-1}$, and thus both conversion matrices are the permutation matrix $\pi_{(132)}$. Then the complete quantum circuit is given by Figure 2.

2.2 Example for $\mathbb{F}_{64}$

Consider $m = 6$ and the finite field $\mathbb{F}_{64}$. Then the primal basis is

$$\{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5\}$$

where α is the primitive root satisfying $\alpha^6 = \alpha + 1$. The matrix A is given by

$$A = \mathrm{Tr}\begin{bmatrix} \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 \\ \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 \\ \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 \\ \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} \\ \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Since $B = A^{-1}$,

$$B = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Hence, the dual basis is given by $\{\alpha^5 + 1, \alpha^4, \alpha^3, \alpha^2, \alpha, 1\}$.

The shift operation of the bit-serial multiplier corresponds to the permutation $\pi_{(234561)}$. For $m = 6$ and x in dual coordinates, the parity tree corresponds to

$$\begin{aligned} \mathrm{Tr}(x\alpha^6) &= x'_1 + x'_0 \\ &= x_4 + x_5 + x_0 \end{aligned}$$

which is derived from duality relationships.

Thus, the bit-serial multiplier transformation BSM is given by

$$\begin{aligned} BSM &= \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \end{aligned}$$

Hence, the quantum circuit diagram for this bit-serial multiplier is given by Figure 3.

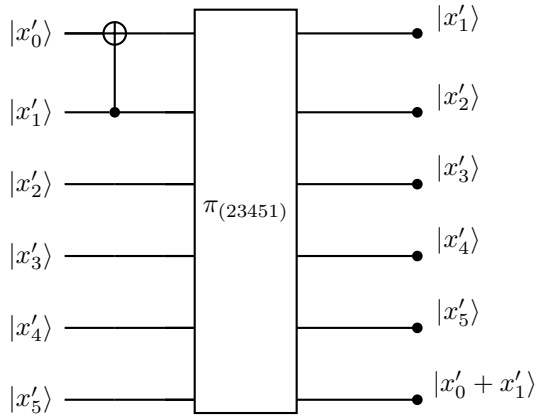

Figure 3: Quantum bit-serial circuit that performs multiplication by the primitive element satisfying $\alpha^6 = \alpha + 1$. Computed in the dual coordinate system.

Now consider the change of basis matrices A and B. To complete the quantum circuit representation, these matrices must be rendered as quantum gates. However, both matrices can be easily decomposed into a CNOT gate and the permutation $\pi_{(654321)}$.

$$A = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$B = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Let $x \in \mathbb{F}_{64}$ be given in primal coordinates. Denote the permutation $\pi_{(234561)}$ by π_0 and the permutation $\pi_{(654321)}$ by π_1. Then multiplication by the primitive element satisfying $\alpha^6 = \alpha + 1$ can be accomplished by the quantum circuit in Figure 4.

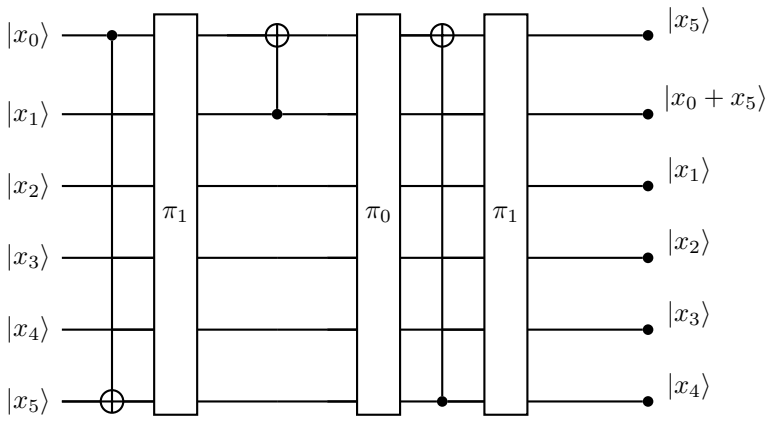

Figure 4: The complete quantum circuit diagram for multiplication by α, where α satisfies $\alpha^6 = \alpha + 1$.

3 Discussion

The examples for $\mathbb{F}_8$ and $\mathbb{F}_{64}$ demonstrate that bit-serial multipliers can be translated to quantum circuits that efficiently perform multiplication by a primitive element. This bit-serial paradigm for multiplication by α offers several advantages to other approaches.

Let BSM denote the CNOT gate and permutation matrix of the bit-serial multiplier. Note that $\mathcal{P} = A \cdot BSM \cdot B$, where $\mathcal{P}$ is the matrix described in Section 1.3 that describes multiplication by α. Hence, the bit-serial multiplier provides a decomposition of $\mathcal{P}$ that is fixed by the choice of irreducible polynomial $p(x)$.

A prior approach to generate a quantum circuit for $\mathcal{P}$ was to perform an LU decomposition, since triangular matrices can be readily represented as CNOT gates. Of course, the LU decomposition has an associated time complexity that becomes expensive as the number of qubits in the system increase. Thus, the dependence of the bit-serial multiplier solely on the primitive polynomial allows the matrices to be computed in advanced, a significant advantage over the LU decomposition method.

Consider the examples described in Section 2.1 and 2.2. The polynomial $p(x) = x^3 + x + 1$ is the ideal case, since the change of basis matrices are permutation matrices, and $p(x) = x^6 + x + 1$ is a straightforward case where the change of basis matrices decompose into a permutation and single CNOT gate. These results naturally lead to the discussion of whether every bit-serial multiplier can be readily converted into quantum circuits. [5] introduces the notion of permutation duals, where the bases $\{\alpha_0, \ldots, \alpha_{m-1}\}$ and $\{\beta_0, \ldots, \beta_{m-1}\}$ are said

Irreducible polynomial	Values of m
$x^m + x + 1$	2, 3, 4, 6, 7, 9, 15, 22, 28, 30, 46, 60, 63, 127, 153, 172, 303, 471, 532, 865, 900

Table 1: Values of m for which there exists an irreducible trinomial of the specified form

to be permutation duals if $\mathrm{Tr}(\alpha_j \beta_k)$ is a permutation matrix. [5] proved that basis change via permutation occurs if and only if the primitive polynomial is a trinomial. [5] explores the implications of permutation duals for classical bit-serial multipliers.

Furthermore, [9] describe the permutation self-dual, where the primal basis is said to be a permutation self-dual basis of $\mathbb{F}_{2^m}$ if and only if α is the root of the irreducible polynomial of the form $x^m + x + 1$ for m odd. Furthermore, although the change of basis matrix cannot be ensured to be a permutation for m even, the sparsity of this matrix can be explicitly determined. Let the weight of a matrix denote the number of entries equal to 1. Since any change of basis matrix must have at least m non-zero entries, we are interested in minimizing the excess relative to m. For even m, the excess is equal to 1 if and only if α is the root of the irreducible polynomial $x^m + x + 1$.

Note that the former case corresponds to Example 2.1, whereas the latter case corresponds to Example 2.2. Recall that the parity tree of the bit-serial multiplier is calculated from $\mathrm{Tr}(x\alpha^m)$. For irreducible polynomials of the form $x^m + x + 1$, $\alpha^m = \alpha + 1$. Thus, the parity tree corresponds to the single CNOT gate $\mathrm{Tr}(x\alpha^m) = x'_1 + x'_0$. For even m, two additional CNOT gates are required for the excess in each change of basis matrix. Hence, when there exists an irreducible polynomial of the form $x^m + x + 1$ for $\mathbb{F}_{2^m}$, one CNOT gate and three permutations are required for odd m, and three CNOT gates and three permutations are required for even m when implementing multiplication by α as a bit-serial multiplier.

However, the polynomial of the form $x^m + x + 1$ is not necessarily irreducible for all fields $\mathbb{F}_{2^m}$. For example, $x^5 + x + 1$ is not irreducible over $\mathbb{F}_{32}$. In fact, $x^m + x + 1$ is irreducible for only 21 values for $m < 1000$. These values are given in Table 1. Hence, there is an interest bounding the gate complexity for a general m. From the construction of the parity tree, it is evident that a trinomial results in the most sparsity. Suppose the trinomial $x^m + x^k + 1$, $m-1 > k > 1$ is irreducible over $\mathbb{F}_{2^m}$. Then the parity tree is $\mathrm{Tr}(x\alpha^m) = x'_k + x'_0$ since $\alpha^m = \alpha^k + 1$. Thus, a general trinomial results in a BSM consisting of a single permutation and CNOT gate. The complexity of the basis conversion matrices is more nuanced. [5] suggests that a permutation dual can be found in an ad hoc manner by appropriately choosing β for every trinomial of interest, and [9] provides an explicit formula for β. However, these bases are with respect to the general bit-serial multiplier described in [5], which is more complex than

the bit-serial paradigm described in [4] and used here. The gate complexity of conversion matrices for a general m is subject to further research.

Since the Kerdock Codes derive a unitary 2-design, efficient implementations of multiplication by a primitive element are desired. Using the bit-serial multiplier paradigm, multiplication by primitive elements can be reduced to choosing a primitive trinomial $p(x)$. Although the sparsity of these implementations is only guaranteed under certain conditions, these results suggest that there exist low gate complexity for quantum implementations for multiplication by α.

References

[1] Trung Can. *The Heisenberg-Weyl Group, Finite Symplectic Geometry and their Applications*. 2018.

[2] Richard Cleve, Debbie Leung, Li Liu, and Chunhao Wang. *Near-linear constructions of exact unitary 2-designs*. 2015.

[3] Richard A. Low. *Pseudo-randomness and Learning in Quantum Computation*. 2010.

[4] Robert J. McEliece. *Finite Fields for Computer Scientists and Engineers*. Springer, 1987. Chapter 8: Trace, Norm, and Bit-Serial Multiplication.

[5] Ian Blake Muzhong Wang. *Bit Serial Multiplication in Finite Fields*. 1990.

[6] J. H. van Lint P. J. Cameron. *Designs, Graphs, Codes and their Links*. London Mathematical Society Student Texts, 1991.

[7] Henry D. Pfister. *Pfister Narrative*. 2018.

[8] Narayanan Rengaswamy, Robert Calderbank, Swanand Kadhe, and Henry D. Pfister. *Synthesis of Logical Clifford Operators via Symplectic Geometry*. 2018.

[9] Douglass R. Stinson. *On Bit-Serial Multiplication and Dual Bases in GF(2^m)*. 1990.

[10] Robert Calderbank Henry D. Pfister Trung Can, Narayanan Rengaswamy. *Kerdock Codes and Unitary 2-Designs*. 2018.

[11] John Watrous. *The Theory of Quantum Information*. Cambridge University Press, 2018.

[12] Zak Webb. *The Clifford group forms a unitary 3-design*. 2015.