Manuscript submitted to
AIMS' Journals
Volume **X**, Number **0X**, XX **200X**

doi:10.3934/xx.xxxxxxx

pp. **X–XX**

NEW QUANTUM CODES FROM METACIRCULANT GRAPHS VIA SELF-DUAL ADDITIVE $\mathbb{F}_4$-CODES

Padmapani Seneviratne

Department of Mathematics, Texas A&M University-Commerce
2600 South Neal Street, Commerce TX 75428, USA

Martianus Frederic Ezerman*

School of Physical and Mathematical Sciences, Nanyang Technological University
21 Nanyang Link, Singapore 637371

(Communicated by the associate editor name)

Abstract. We use symplectic self-dual additive codes over $\mathbb{F}_4$ obtained from metacirculant graphs to construct, for the first time, $[\![\ell, 0, d]\!]$ qubit codes with parameters $(\ell, d) \in \{(78, 20), (90, 21), (91, 22), (93, 21), (96, 22)\}$. Secondary constructions applied to the qubit codes result in many new qubit codes that perform better than the previous best-known.

1. Introduction.

We work on three closely connected objects, namely, a *metacirculant graph* G, a *symplectic self-dual additive code* C over $\mathbb{F}_4$, and its corresponding *quantum stabilizer code* Q. The route is straightforward. Let I be the identity matrix of a suitable dimension and ω be a root of $x^2 + x + 1 \in \mathbb{F}_2[x]$. We search for a G whose adjacency matrix $A(G)$ leads to C, which is generated by the row span of $A(G) + \omega I$. This code C, in turn, yields Q via the stabilizer method.

For lengths $\ell \in \{27, 36\}$ exhaustive searches are feasible, allowing us to construct some families of additive codes that contain some code C with a higher minimum distance than the best that circulant graphs can lead to. For lengths $\ell \in \{78, 90, 91, 93, 96\}$ we run randomized non-exhausted searches to come up with the new additive codes. We exhibit numerous instances when the resulting qubit codes have better parameters than the best-known comparable quantum codes.

The general construction of quantum stabilizer codes, wherein classical codes are used to describe the quantum error operators, is well-established. Our main reference for the qubit case is the seminal work of Calderbank, Rains, Shor, and Sloane in [4]. Two recent introductory expositions can be found in [7] and [9].

To get to metacirculant graphs, we recall *circulant graphs*, which have been more extensively studied. A recent survey on the subject can be found in [15]. The following definition of circulant graphs is given in [2].

2020 *Mathematics Subject Classification.* Primary: 94B25, 81P73; Secondary: 05C75.

Key words and phrases. additive codes, graph codes, metacirculant graph, quantum codes, self-dual codes.

Nanyang Technological University Grant Number 04INS000047C230GRT01 supports the research carried out by M. F. Ezerman.

* Corresponding author: Martianus Frederic Ezerman.

Definition 1.1. Let $\mathbb{Z}_n$ denote the ring of integers modulo n and let

$$\mathbb{Z}_n^* := \{x \in \mathbb{Z}_n : 0 < x \leq n/2\}.$$

The circulant graph $\Gamma_n(S)$ is the graph with the vertex set $\mathbb{Z}_n$ where any two vertices x and y are adjacent if and only if $|x-y|_n \in S$, with $S \subseteq \mathbb{Z}_n^*$ and

$$\begin{cases} |a|_n := a & \text{if } 0 \leq a \leq n/2, \\ |a|_n := n-a & \text{if } n/2 < a < n. \end{cases}$$

The adjacency matrix of a circulant graph is a *circulant matrix*. An $n \times n$ matrix A is circulant if it has the form

$$A = \begin{pmatrix} a_1 & a_2 & \cdots & a_{n-1} & a_n \\ a_n & a_1 & \cdots & a_{n-2} & a_{n-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_3 & a_4 & \cdots & a_1 & a_2 \\ a_2 & a_3 & \cdots & a_n & a_1 \end{pmatrix}. \tag{1}$$

If the adjacency matrix $A := A(G)$ of G is circulant, then $a_1 = 0$ and $a_i = a_{n+2-i}$ for $i \in \{2, \ldots, \lfloor n/2 \rfloor\}$. Circulant matrices are used as building blocks in the constructions of many different classes of codes. Examples include self-dual codes, cyclic codes, and quadratic residue codes.

Circulant graphs are *vertex transitive* [2]. They are the Cayley graphs of $\mathbb{Z}_n$. In 1982, Alspach and Parsons [1] constructed a family of vertex transitive graphs. Each graph in the family has a transitive permutation group as a subgroup of its automorphism group. They named the family *metacirculant graphs* as it contains the class of circulant graphs.

Li, Song, and Wang in [13, Definition 1.1], following D. Marušič in [14], call a graph $\Gamma = (V, E)$ an (m,n)-metacirculant if $|V| = mn$ and Γ has two automorphisms ρ and σ that satisfy some conditions. First, $\langle \rho \rangle$ is semiregular and has m orbits on V. Second, σ cyclically permutes the m orbits of $\langle \rho \rangle$ and normalizes $\langle \rho \rangle$. Third, σ^m fixes at least one vertex of Γ. In this work, we follow an equivalent combinatorial definition.

Definition 1.2. ([1]) Let m, n be two fixed positive integers and $\alpha \in \mathbb{Z}_n$ be a unit. Let $S_0, S_1, \ldots, S_{\lfloor m/2 \rfloor} \subseteq \mathbb{Z}_n$ satisfy the four properties

1. $S_0 = -S_0$.
2. $0 \notin S_0$.
3. $\alpha^m S_k = S_k$ for $1 \leq k \leq \lfloor m/2 \rfloor$.
4. If m is even then $\alpha^{m/2} S_{m/2} = -S_{m/2}$.

The meta-circulant graph $\Gamma := \Gamma\left(m, n, \alpha, S_0, S_1, \ldots, S_{\lfloor m/2 \rfloor}\right)$ has the vertex set $V(\Gamma) = \mathbb{Z}_m \times \mathbb{Z}_n$. Let $V_0, V_1, \ldots, V_{m-1}$, where $V_i := \{(i,j) : 0 \leq j \leq n-1\}$, be a partition of $V(\Gamma)$. Let $1 \leq k \leq \lfloor m/2 \rfloor$. Vertices (i,j) and $(i+k, h)$ are adjacent if and only if $(h-j) \in \alpha^i S_k$.

Henceforth, we let $m > 1$ since a metacirculant graph with $m = 1$ is circulant.

Example 1. The Petersen graph is $\Gamma(2, 5, 2, \{1,4\}, \{0\})$. The vertices are partitioned into

$$V_0 := \{(0,0), (0,1), (0,2), (0,3), (0,4)\} \text{ and } V_1 := \{(1,0), (1,1), (1,2), (1,3), (1,4)\}.$$

Vertices $(0,j)$ and $(0,h)$ are adjacent for $h - j \in S_0$. Vertices $(1,j)$ and $(1,h)$ are adjacent when $h - j \in \{2,3\}$. Vertices $(0,j)$ and $(1,j)$ are adjacent for $0 \leq j \leq 4$.

Figure 1, typeset in `TikZ-network` [12], relabels the vertices lexicographically. The upper layer contains the vertices in V_0 as $1, \dots, 5$ while the lower layer presents the vertices in V_1 as $6, \dots, 10$.

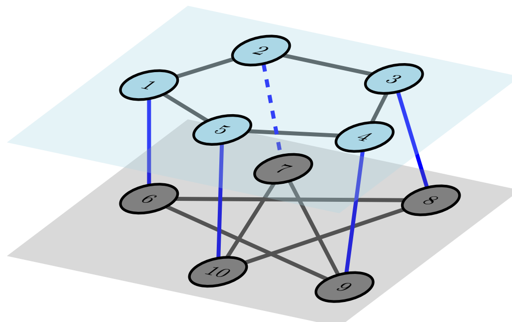

FIGURE 1. The Petersen Graph as $\Gamma(2, 5, 2, \{1, 4\}, \{0\})$.

The following fact is well-known.

Theorem 1.3. ([1]) *Let $\phi(\cdot)$ denote the Euler totient function. If* $\gcd(m, n) = 1$ *and* $\gcd(m, \phi(n)) = 1$, *then the metacirculant* $\Gamma\left(m, n, \alpha, S_0, S_1, \dots, S_{\lfloor m/2 \rfloor}\right)$ *is isomorphic to a circulant graph.*

The next lemma determines the degree of each vertex.

Lemma 1.4. *Any* $G := \Gamma\left(m > 1, n, \alpha, S_0, S_1, \dots, S_{\lfloor m/2 \rfloor}\right)$ *is regular. The degree of each vertex is given by*

$$\begin{cases} |S_0| + |S_1| & \text{if } m = 2, \\ |S_0| + |S_{\lfloor m/2 \rfloor}| + 2\left(\sum_{r=1}^{\lfloor m/2 \rfloor - 1} |S_r|\right) & \text{if } m \geq 4 \text{ is even,} \\ |S_0| + 2\left(\sum_{r=1}^{\lfloor m/2 \rfloor} |S_r|\right) & \text{if } m \geq 3 \text{ is odd.} \end{cases} \tag{2}$$

Proof. Since the automorphism group of G acts transitively on its vertices, G is a regular graph. Hence, it suffices to determine the degree of vertex $(0, 0) \in V_0$. The vertex is adjacent to a vertex $(0, h) \in V_0$ if and only if $h \in S_0$. This implies that $(0, 0)$ is adjacent to $|S_0|$ vertices in V_0.

Next, $(0, 0)$ is adjacent to a vertex $(k, h) \in V_k$ if and only if $h \in S_k$. Hence, $(0, 0)$ is adjacent to $|S_k|$ vertices in V_k. The set S_k determines the edges between layers V_0 and V_k whose indices differ by k for $1 \leq k \leq \lfloor m/2 \rfloor$. When m is odd, the index 0 of V_0 differs by k from both the indices k and $m - k$ of V_k and V_{m-k} for all $1 \leq k \leq \lfloor m/2 \rfloor$. When m is even, $V_{m/2} = -V_{m/2}$, which implies that the index 0 of V_0 differs by k from both the indices k and $m - k$ of V_k and V_{m-k} for all $1 \leq k \leq \lfloor m/2 \rfloor - 1$. Thus, the degree of vertex $(0, 0)$ is as given in Equation 2. □

Theorem 1.5. *Let* $S := \left\{S_0, S_1, \dots, S_{\lfloor m/2 \rfloor}\right\}$. *Given the graph* $G := \Gamma(m, n, \alpha, S)$, *let* $\{V_i : i \in \{0, 1, \dots, m-1\}\}$, *with* $V_i := \{(i, j) : 0 \leq j < n\}$, *be the partition of the vertex set into m layers, each containing n vertices. Then G is a multi-partite metacirculant graph with m partitions if and only if S_0 is the empty set.*

Proof. By Definition 1.2, two vertices (i, j) and $(i+k, h)$ are adjacent in $\Gamma(m, n, \alpha, S)$ if and only if $h - j \in \alpha^i\, S_k$. Both vertices are in the same layer V_i whenever $k = 0$.

Hence, the two vertices (i,j) and (i,h) in V_i are adjacent if and only if $h-j \in \alpha^i\, S_0$. The set S_0 being empty implies $h-j \notin \alpha^i\, S_0$. Thus, there is no edge between any pair of vertices within the same layer V_i. □

2. **Self-dual additive codes from metacirculant graphs.** A code over $\mathbb{F}_4 := \{0,1,\omega,\overline{\omega}=\omega^2=1+\omega\}$ is said to be *additive* if it is $\mathbb{F}_2$-linear, *i.e.*, the code is closed under addition but closure under multiplication by the elements in $\mathbb{F}_4 \setminus \mathbb{F}_2$ is not required. An $\mathbb{F}_4$-linear code is additive. An element $\mathbf{c}$ of C is called a codeword of C. The *weight* of $\mathbf{c}$ is the number of nonzero entries that it has. The *minimum distance* of C is the least nonzero weight of all codewords in C. If C is an additive code of length ℓ over $\mathbb{F}_4$, of size 2^k and minimum distance d, then we denote C by $(\ell,2^k,d)_4$. Let $W_i := W_i(C)$ be the number of codewords of weight i in C. Then the set $\{W_0,W_1,\ldots,W_n\}$ is the *weight distribution* of C. It is convenient to express the weights as a polynomial out of the W_is. The *weight enumerator* of C is the polynomial $W_C(y) = W_0 + W_1 y + \ldots + W_n y^n$.

The *trace Hermitian inner product* of $\mathbf{x} = (x_1,\ldots,x_n)$ and $\mathbf{y} = (y_1,\ldots,y_n)$ in $\mathbb{F}_4^n$ is given by

$$\mathbf{x} * \mathbf{y} = \sum_{j=1}^{n} \left(x_j y_j^2 + x_j^2 y_j\right). \tag{3}$$

Given an additive code C, its *symplectic dual* C^* is

$$C^* = \{\mathbf{x} \in \mathbb{F}_4^n : \mathbf{x} * \mathbf{c} = 0 \text{ for all } \mathbf{c} \in C\}$$

and C is said to be *(symplectic) self-dual* if $C = C^*$.

An additive $\mathbb{F}_4$ self-dual code is called *Type II* if all of its codewords have even weights. A code which is not Type II is called *Type I*. It is well-known that Type II codes must have even lengths.

Self-dual codes, under various inner products and possible alphabet sets, have been extensively studied due to their rich algebraic, combinatorial, and geometric structures. A major reference on this topic is the book [16] authored by Nebe, Rains, and Sloane. Of particular relevance to our family of additive self-dual codes here, labeled as family 4^{H+} in [16], is the treatment in Section 6 of Chapter 7 and in Chapter 11.

Let $A(\Gamma)$ be the adjacency matrix of the graph Γ and I be the identity matrix. The following nice result was first shown by Schlingemann in [18] and subsequently discussed in [5, Section 3]. Every graph represents a self-dual additive code over $\mathbb{F}_4$ and every self-dual additive code over $\mathbb{F}_4$ can be represented by a graph. In particular, the additive $\mathbb{F}_4$-code $C := C(\Gamma)$ generated by the row span of the matrix $A(\Gamma) + \omega I$ is symplectic self-dual.

Danielsen and Parker gave a complete classification of *all* self-dual additive codes over $\mathbb{F}_4$ for $n \leq 12$ in [5]. Follow-up works, covering $n \leq 50$, were contributed by Gulliver and Kim in [11], by Varbanov in [19], by Grassl and Harada in [10], and by Saito in [17]. Their collective efforts focused on codes derived from graphs whose adjacency matrices are either *circulant* or *bordered circulant*. Our work here expands the search for new qubit codes by exploring metacirculant graphs. The following result classifies Type I and Type II additive $\mathbb{F}_4$ self-dual codes generated by metacirculant graphs.

Theorem 2.1. *Let C be an additive $\mathbb{F}_4$ self-dual code generated by*

$$\Gamma\left(m,n,\alpha,S_0,S_1,\ldots,S_{\lfloor m/2 \rfloor}\right), \text{ with } 2 \mid (mn).$$

Let

$$\Delta_S := \begin{cases} |S_0| & \text{if } m \text{ is odd,} \\ |S_0| + |S_{\lfloor m/2 \rfloor}| & \text{if } m \text{ is even.} \end{cases} \tag{4}$$

Then C is Type II if and only if Δ_S is odd.

Proof. Let mn be even. An additive self-dual $\mathbb{F}_4$ code $C = C(\Gamma)$ is Type II if and only if all vertices of Γ have odd degree [5]. Lemma 1.4 gives the degree of each vertex in $\Gamma\left(m, n, \alpha, S_0, S_1, \ldots, S_{\lfloor m/2 \rfloor}\right)$. By Equation 2, the degree is odd if and only if Δ_S is odd. □

The three parameters of a qubit code $Q \subseteq \mathbb{C}^{2^\ell}$ are its *length* ℓ, *dimension* K over $\mathbb{C}$, and *minimum distance* $d = d(Q)$. The notation

$$((\ell, K, d)) \text{ or } [\![\ell, k, d]\!] \text{ with } k = \log_2 K$$

signifies that Q encodes k logical qubits as ℓ physical qubits, with d being the smallest number of simultaneous quantum error operators that can send a valid codeword into another.

A symplectic self-dual additive code C over $\mathbb{F}_4$ of length ℓ and minimum distance d gives an $[\![\ell, 0, d]\!]_2$ qubit code Q. Since $k = 0$, that is the code Q consists of a single quantum state, one needs to carefully interpret the meaning of minimum distance. As explained in [4, Section III], an $[\![\ell, 0, d]\!]$ code Q has the property that, when subjected to a decoherence of $\lfloor (d-1)/2 \rfloor$ coordinates, it is possible to *determine exactly* which coordinates were decohered. This code can be used, for example, to test if certain storage locations for qubits are decohering faster than they should.

Such a code Q can be of interest in their own right. An example is the unique $[\![2, 0, 2]\!]$ code that corresponds to the maximally entangled quantum state known as the EPR pair in the famed paper [6] of Einstein, Podolsky, and Rosen. More commonly, a zero-dimensional code is used as a seed in some secondary constructions of quantum codes to produce qubit codes with $k > 0$.

Theorem 2.2. [4, Theorem 6] *Assume that a qubit $((\ell, K, d > 1))_2$ code Q exists. Then the following qubit codes exist. An $((\ell, K', d))_2$ code for all $1 < K' \leq K$ by subcode construction. A $((\lambda, K, d))_2$ code for all $K > 1$ and $\lambda \geq \ell$ by lengthening. An $((\ell - 1, K, d - 1))_2$ code by puncturing.*

There is also a quantum analogue of the *shortening* construction on classical code, although the former is less straightforward to perform. Interested reader can consult [9, Section 4.3] for the procedure.

Example 2. The $[12, 6, 6]_4$ `dodecacode` $\mathcal{D}$ yields the unique $[\![12, 0, 6]\!]$ qubit code. It can be generated by the metacirculant graph $G_{12} := \Gamma(2, 6, 5, \{3\}, \{0, 3, 4, 5\})$. Figure 2 shows G_{12} with the vertices relabeled for convenience. The `dodecacode` is Type II, with weight enumerator $1 + 396y^6 + 1485y^8 + 1980y^{10} + 234y^{12}$.

Many known optimal or currently best-performing qubit codes of length ℓ with $K = 1$ in the literature, *i.e.*, $[\![\ell, 0, d]\!]_2$ with best-known or optimal d, are constructed based on circulant graphs [5, 10, 17]. We will soon show that strict improvements can be gained when one starts with metacirculant graphs. We use `MAGMA` [3] for all computations.

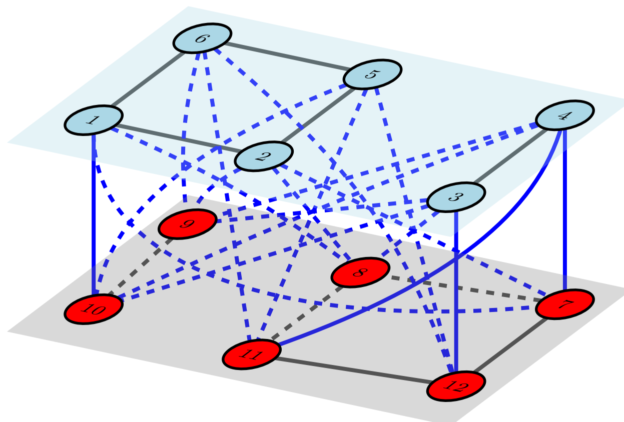

FIGURE 2. $G_{12} := \Gamma(2, 6, 5, \{3\}, \{0, 3, 4, 5\})$ of the `dodecacode` $\mathcal{D}$. □

3. Higher best-known minimum distances of additive symplectic self-dual codes.

This section presents additive symplectic self-dual codes of length $\ell \in \{27, 36\}$ with stricly higher minimum distances than any that can be derived from circulant graphs. The strict improvements, however, do not extend to the quantum setup. There are $[\![\ell, 0, d]\!]$ qubit codes, constructed from other approaches as recorded in the corresponding entries in [8], whose minimum distances are equal to the ones that we derive here.

For length $\ell = 27$, Varbanov in [19] concluded after an exhaustive search that the circulant graph construction only yields additive self-dual codes $\left(27, 2^{27}, \widehat{d}\right)_4$ of highest minimum distance $d = 8 \geq \widehat{d}$. Using the metacirculant graph construction, we obtain additive self-dual codes with parameters $\left(27, 2^{27}, 9\right)_4$. They yield $[\![27, 0, 9]\!]$ qubit codes, which meet the best-known parameters in [8].

Proposition 1. *There are two inequivalent families of* $\left(27, 2^{27}, 9\right)_4$ *additive self-dual codes from metacirculant graphs with* $(m, n) = (3, 9)$*. Each family consists of* 108 *equivalent codes. They yield* $[\![27, 0, 9]\!]$ *qubit stabilizer codes.*

Proof. An exhaustive search found 216 metacirculant graphs $\{\Gamma(3, 9, \alpha, S_0, S_1)\}$ in two non-isomorphic families, which we call $\mathcal{F}_{27,1}$ and $\mathcal{F}_{27,2}$, corresponding to two inequivalent codes $C_{27,1}$ and $C_{27,2}$. The respective families can be represented by the graphs

$$G_{27,1} := \Gamma(3, 9, 4, \{2, 7\}, \{0, 1, 2, 3, 4, 5, 8\}) \text{ and}$$
$$G_{27,2} := \Gamma(3, 9, 7, \{1, 3, 6, 8\}, \{0, 5, 8\}). \tag{5}$$

To confirm that the resulting codes are inequivalent, it suffices to note that the number of weight 9 words are 591 and 717, respectively. We note that both codes have $W_i > 0$ for all $9 \leq i \leq 27$. When i is even, $W_i(C_{27,1}) = W_i C_{27,2}$.

The complete list of the 216 metacirculant graphs, divided into the families $\mathcal{F}_{27,1}$ and $\mathcal{F}_{27,2}$, and the weight distributions of the two inequivalent codes can be found in the supplementary material. □

A self-dual additive $\left(36, 2^{36}, 12\right)_4$ code from circulant graphs does *not* exist, since the best minimum distance is confirmed to be 11 in [10, 17]. The metacirculant graph construction increases the known minimum distance of length 36 additive self-dual codes to 12.

Proposition 2. *There are* 72 *metacirculant graphs with* $(m,n)=(2,18)$*, producing two inequivalent additive symplectic self-dual* $\left(36,2^{36},12\right)_4$ *Type* II *codes. We can separate the* 72 *graphs into two families, which we call* $\mathcal{F}_{36,1}$ *and* $\mathcal{F}_{36,2}$*. Each family consists of* 36 *isomorphic graphs. They yield* $[\![36,0,12]\!]$ *qubit codes. The respective families can be represented by the graphs*

$$\begin{aligned} G_{36,1} &:= \Gamma(2,18,1,\{4,6,12,14\},\{3,4,6,7,9,11,12,14,15\}),\\ G_{36,2} &:= \Gamma(2,18,1,\{4,6,12,14\},\{1,4,7,8,9,10,11,14,17\}). \end{aligned} \tag{6}$$

Proof. The weight distributions of the additive self-dual codes $C_{36,1}$ and $C_{36,2}$ derived, respectively, from $G_{36,1}$ and $G_{36,2}$ confirm that the codes are Type II. We have $W_i>0$ for $i\in\{0\}\cup\{2j:6\leq j\leq 18\}$. The two additive codes are inequivalent since $W_{12}(C_{36,1})=28764\neq 20844=W_{12}(C_{36,2})$. The list of $\{\alpha,S_0,S_1\}$ for the metacirculant graphs $\Gamma(2,18,\alpha,S_0,S_1)$ that splits into two families can be found in the supplementary material. The graphs $G_{36,1}$ and $G_{36,2}$ share a common structure when we look into edges that are incident to vertices within the same layer. The structures differ only on the edges that are incident to vertices that belong to two distinct layers. □

4. **New qubit codes.** Here we present new qubit codes $[\![\ell,0,d]\!]_2$ for lengths $\ell\in\{78,90,91,93,96\}$. Due to the large sizes of the relevant graphs, we supply a `MAGMA` routine to generate them in the supplementary material instead of presenting the graphs explicitly. For each ℓ, we keep a record of the minimum distance calculation and include it as a supporting document.

Applying secondary constructions yields more qubit codes with strictly better parameters that previously known. There are computational routines used by M. Grassl to perform the propagation rules on the improved codes submitted for inclusion to his online table [8]. We highlight the process only for $\ell=78$, for brevity.

Proposition 3. *The metacirculant graph*

$$\begin{aligned} G_{78} := \Gamma(6,13,12,&\{1,4,6,7,9,12\},\{1,2,3,5,7,8,9,11\},\\ &\{1,2,4,5,8,10\},\{1,2,3,6,7,8,12\}) \end{aligned} \tag{7}$$

yields a new $\left(78,2^{78},20\right)_4$ *Type II additive self-dual code. The corresponding* Q_{78} *is a new* $[\![78,0,20]\!]$ *qubit code. Prior to our discovery, the best-known was* $[\![78,0,19]\!]$ *and the first known occurence of* $d=20$ *was at* $\ell=80$*. Our new qubit code has been listed as the current best-known since October 13, 2020 in Grassl's table* [8] *based on a private communication.*

Proof. A randomized search in `MAGMA` found G_{78}. The graph yields the self-dual additive code C_{78} of distance $d=20$. By Theorem 2.1, $\Delta_S=|S_0|+|S_3|=13$, which implies that C_{78} is Type II. The qubit code Q_{78} can then be certified to have the claimed parameters. □

By propagation rules, strict improvements have also been achieved by puncturing, shortening, lengthening, and taking a subcode of Q_{78}. Table 1 provides the details.

Table 1. New codes from modifying Q_{78}

Code	Parameters	Propagation rule
$Q_{78,1}$	$[\![77,0,19]\!]_2$	Puncture Q_{78} at $\{78\}$
$Q_{78,2}$	$[\![77,1,19]\!]_2$	Shorten Q_{78} at $\{78\}$
$Q_{78,3}$	$[\![78,1,19]\!]_2$	Lengthen $Q_{78,2}$ by 1
$Q_{78,4}$	$[\![76,2,18]\!]_2$	Shorten Q_{78} at $\{77,78\}$
$Q_{78,5}$	$[\![76,1,18]\!]_2$	Subcode of $Q_{78,4}$
$Q_{78,6}$	$[\![77,2,18]\!]_2$	Lengthen $Q_{78,4}$ by 1
$Q_{78,7}$	$[\![75,3,17]\!]_2$	Shorten Q_{78} at $\{76,77,78\}$
$Q_{78,8}$	$[\![76,3,17]\!]_2$	Lengthen $Q_{78,7}$ by 1
$Q_{78,9}$	$[\![75,2,17]\!]_2$	Subcode of $Q_{78,7}$

Proposition 4. *The metacirculant graph*

$$G_{90} := \Gamma(10,9,8,\{1,8\},\{0,1,2,4,5,8\},\{5,6\},\\ \{2,4,5,6,8\},\{0,1,2,4,7\},\{0,5,7,8\}) \quad (8)$$

generates a new $\left(90,2^{90},21\right)_4$ *Type I additive self-dual code* C_{90}*. The new* $[\![90,0,21]\!]$ *qubit code* Q_{90} *has better minimum distance than the best-known* $[\![90,0,20]\!]$ *in* [8].

Proof. The graph G_{90} and the resulting codes C_{90} and Q_{90} as well as their parameters were found by MAGMA searches. The code C_{90} is Type I by Theorem 2.1, since $\Delta_S = |S_0| + |S_5| = 6$. □

Proposition 5. *The multi-partite metacirculant graph*

$$G_{91} := \Gamma(7,13,3,\{\},\{4,7,8,10,11,12\},\\ \{1,3,4,7,8,9,10,11,12\},\{0,4,7,8,10,11,12\}) \quad (9)$$

gives a new $\left(91,2^{91},22\right)_4$ *Type I additive self-dual code* C_{91}*. The new* $[\![91,0,22]\!]$ *qubit code* Q_{91} *has better minimum distance than the* $[\![91,0,21]\!]$ *code in* [8].

Proof. By Theorem 1.5, G_{91} is a multi-partite graph. The vertices are partitioned into 7 layers, each containing 13 vertices. We used MAGMA to verify that the minimum distance d of the generated $(91,2^{91},d)_4$ self-dual additive code C_{91} is indeed 22. This code is clearly Type I since its length is odd. The corresponding $[\![91,0,22]\!]$ qubit code Q_{91} improves on the $[\![91,0,21]\!]$ code currently listed as best-known in [8]. □

Proposition 6. *The metacirculant graph*

$$G_{93} := \Gamma(3,31,1,\{10,12,14,15,16,17,19,21\},\\ \{2,7,8,10,11,13,15,16,17,19\}) \quad (10)$$

generates a new $\left(93,2^{93},21\right)_4$ *additive self-dual code* C_{93}*. The code is Type I due to its odd length. The new* $[\![93,0,21]\!]$ *qubit code* Q_{93} *has better minimum distance when compared with the prior best-known* $[\![93,0,20]\!]$ *qubit code in* [8].

Proof. We used MAGMA to verify that the generated $\left(93,2^{93},d\right)_4$ additive self-dual code C_{93} has minimum distance $d = 21$. The code corresponds to a new $[\![93,0,21]\!]$ qubit code Q_{93}. □

TABLE 2. Properties of the Graphs

G	$d_{\min}(G)$	$\nu(G)$	$\gamma(G)$	$\lvert\mathrm{Aut}(G)\rvert$	G	$d_{\min}(G)$	$\nu(G)$	$\gamma(G)$	$\lvert\mathrm{Aut}(G)\rvert$
G_{12}	6	5	4	24	G_{78}	20	41	7	78
$G_{27,1}$	9	16	6	27	G_{90}	21	42	7	90
$G_{27,2}$	9	10	4	27	G_{91}	22	44	7	546
$G_{36,1}$	12	13	6	72	G_{93}	22	28	4	186
$G_{36,2}$	12	13	4	72	G_{96}	22	35	6	96

Proposition 7. *The metacirculant graph*

$$G_{96} := \Gamma(6, 16, 7, \{2, 4, 6, 7, 9, 10, 12, 14\}, \{1, 3, 4, 5, 7, 9, 10\}, \{3, 5, 11, 14\}, \{0, 2, 7, 10, 15\}) \quad (11)$$

generates a new $\left(96, 2^{96}, 22\right)_4$ *Type II additive self-dual code* C_{96}*. The new* $[\![96, 0, 22]\!]$ *qubit code* Q_{96} *improves the minimum distance of the prior best-known* $[\![96, 0, 20]\!]$ *code in* [8].

Proof. We confirmed that the minimum distance of C_{96} is 22 by using MAGMA. Since $\Delta_S = |S_0| + |S_3| = 13$, the code is Type II by Theorem 2.1. □

5. **Concluding Remarks.** There are at least two challenging aspects in finding improved symplectic self-dual additive codes over $\mathbb{F}_4$ or strictly better qubit codes. First, the search space quickly widens as the length ℓ grows. Second, determining the minimum distances of the codes is computationally expensive [20]. On a laptop with 11.6 GB available memory, powered by an Intel i7-7500U CPU, a single core run of MAGMA found the minimum distance for the code in Proposition 3 in 10 hours. For the code in Proposition 7, the computation took 41 days and 15 hours.

We have shown that focusing on metacirculant graphs which are not isomorphic to the circulant ones is a fruitful approach. Bringing this work to its end, Table 2 summarizes the properties of the graphs that we have used above. All of them have diameter 2 and girth 3. Included in the table, for each graph G, are the minimum distance $d_{\min}(G)$ of the generated additive code $C := C(G)$, the degree $\nu(G)$ of each vertex in G, the size $\gamma(G)$ of the maximum clique, and the size $|\mathrm{Aut}(G)|$ of the automorphism group of G.

Acknowledgements. We thank the editor and the two anonymous reviewers for their scrutiny of our initial submission. Their thoughtful assessment and critical suggestions help us to improve our work considerably.

Supplementary Material.

1. The graphs, their properties, and the corresponding additive codes can be explicitly constructed by running `record.m`. Included in the output are the complete weight enumerators of the codes of lengths $\ell \in \{12, 27, 36\}$.
2. The relevant graphs with 27 vertices are split into families $\mathcal{F}_{27,1}$ and $\mathcal{F}_{27,2}$ by `families27.m`. Those with 36 vertices are separated into families $\mathcal{F}_{36,1}$ and $\mathcal{F}_{36,2}$ by `families36.m`.
3. The respective five certificates of the minimum distance computations are labelled `78_20.txt`, `90_21.txt`, `91_22.txt`, `93_21.txt`, and `96_22.txt`.

REFERENCES

[1] B. Alspach and T. D. Parsons, A construction for vertex-transitive graphs, *Canad. J. Math.*, **34** (1982), 307–318.
[2] Zbigniew R. Bogdanowicz, Pancyclicity of connected circulant graphs, *J. Graph Theory*, **22** (1996), 167–174.
[3] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system I: The user language, *J. Symb. Comput.*, **24** (1997), 235–265.
[4] A. R. Calderbank, E. M. Rains, P. M. Shor and N. J. A. Sloane, Quantum error correction via codes over $GF(4)$, *IEEE Trans. Inform. Theory*, **44** (1998), 1369–1387.
[5] L. E. Danielsen and M. G. Parker, On the classification of all self-dual additive codes over $GF(4)$ of length up to 12, *J. Combin. Theory, Ser. A*, **113** (2006), 1351–1367.
[6] A. Einstein, B. Podolsky, and N. Rosen, Can quantum-mechanical description of physical reality be considered complete?, *Phys. Rev.*, **47** (1935), 777–780.
[7] Martianus F. Ezerman, Quantum error-control codes, Chapter 27 in W. C. Huffman, J.-L. Kim and P Solé (Eds.), *Concise Encyclopedia of Coding Theory*, 1^{st} edition, Chapman and Hall (CRC Press), Boca Raton, 2021.
[8] Markus Grassl, Bounds on the minimum distance of linear codes and quantum codes. Online available at http://www.codetables.de, 2007, accessed on 2021-04-30.
[9] Markus Grassl, Algebraic quantum codes: Linking quantum mechanics and discrete mathematics, *Int. J. Comput. Math.: Comput. Syst. Theory*, (2020) DOI: 10.1080/23799927.2020.1850530
[10] M. Grassl and M. Harada, New self-dual additive $\mathbb{F}_4$-codes constructed from circulant graphs, *Discrete Math.*, **340** (2017), 399–403.
[11] T. A. Gulliver and J-L. Kim, Circulant based extremal additive self-dual codes over $GF(4)$, *IEEE Trans. Inform. Theory*, **50** (2004), 359–366.
[12] Jürgen Hackl, TikZ-network manual, preprint, arXiv:1709.06005. Source code at https://github.com/hackl/tikz-network.
[13] C. H. Li, S. J. Song and D. J. Wang, A characterization of metacirculants, *J. Combin. Theory, Ser. A*, **120** (2013), 39–48.
[14] Dragan Marušič, On 2-arc-transitivity of Cayley graphs, *J. Combin. Theory, Ser. B*, **87** (2003), 162–196. Corrigendum in *J. Combin. Theory, Ser. B*, **96** (2006), 761–764.
[15] Èmiliya A. Monakhova, A survey on undirected circulant graphs, *Discrete Math. Algorithms Appl.*, **04** (2012), 1250002.
[16] G. Nebe, E. M. Rains and N. J. A. Sloane, *Self-Dual Codes and Invariant Theory*, Springer, Berlin, Heidelberg, 2006.
[17] Ken Saito, Self-dual additive $\mathbb{F}_4$-codes of lengths up to 40 represented by circulant graphs, *Adv. Math. Commun.*, **13** (2019), 213–220.
[18] Dirk Schlingemann, Stabilizer codes can be realized as graph codes, *Quantum Info. Comput.*, **2** (2002), 1533–7146.
[19] Zlatko Varbanov, Additive circulant graph codes over $GF(4)$, *Math. Maced.*, **6** (2008), 73–79.
[20] Alexander Vardy, The intractability of computing the minimum distance of a code, *IEEE Trans. Inform. Theory*, **43** (1997), 1757–1766.

Received xxxx 20xx; revised xxxx 20xx.

E-mail address: Padmapani.Seneviratne@tamuc.edu
E-mail address: fredezerman@ntu.edu.sg