ODD WEIGHT AND THE DIMENSION OF AN ABELIAN BICYCLE CODE: $k \neq 2$, $k = 4$ FORCES $3 \mid \exp G$, AND $k = 6$ FORCES $7 \mid \exp G$

KOREA SUPERINTELLIGENCE LABS

ABSTRACT. For a finite abelian group G and $A, B \in \mathbb{F}_2[G]$, the bicycle code of the pair (A, B) is the CSS code on $n = 2|G|$ qubits with check matrices $H_X = (A\ B)$ and $H_Z = (B^{\mathsf{T}}\ A^{\mathsf{T}})$. Surveying more than 170 three-factor tori with weight-3 polynomials, Galimova observed that $k = 6$ occurs only when 7 divides the exponent of the group, gave a partial explanation, and wrote that "what remains unproven is whether other algebraic mechanisms … can also yield $k = 6$". We prove the statement, in a form that mentions neither weight 3, nor the number of cyclic factors, nor any bound on $|G|$: if one of A, B has odd weight, then $k \neq 2$, $k = 4$ forces $3 \mid \exp G$, and $k = 6$ forces $7 \mid \exp G$. The first of the three was reported by Lin and Pryadko as an unexplained empirical absence, and is proved here. The mechanism is the parity of the weight. Odd weight makes the augmentation of A equal to 1, so the quotient algebra $Q = \mathbb{F}_2[G]/(A, B)$, whose dimension is $k/2$, admits no $\mathbb{F}_2$-algebra homomorphism to $\mathbb{F}_2$; and a commutative unital $\mathbb{F}_2$-algebra with no such homomorphism is never 1-dimensional, is $\mathbb{F}_4$ in dimension 2 and $\mathbb{F}_8$ in dimension 3 — a statement about 1, 4 and 64 multiplication tables that we settle by enumeration in place of Artinian structure theory. Reading the conclusion back through the images of G produces an element of order 3 or 7. For cyclic G the same three conclusions are obtained along a second, independent route, over the published dimension formula $k = 2 \deg \gcd(a, b, x^\ell - 1)$ of Panteleev and Kalachev, and are machine-checked for all ℓ at once. We accompany the theorem with an exhaustive census of weight-3 pairs over 30 presentations of abelian groups of order at most 56 — 9 959 476 normalised pairs standing for 2 770 442 265 unnormalised ones — which shows that neither divisibility implication reverses: $\mathbb{Z}_2^3 \times \mathbb{Z}_7$ is seven-divisible and carries no $k = 6$ weight-3 code, while $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_7$ and $\mathbb{Z}_8 \times \mathbb{Z}_7$ of the same order do, and $\mathbb{Z}_2^2 \times \mathbb{Z}_6$ is three-divisible and carries no $k = 4$ one.

1. INTRODUCTION

The objects. Let G be a finite abelian group, written additively, of order $N = |G|$, and let $R = \mathbb{F}_2[G]$ be its group algebra. We identify $A \in R$ with its support $\operatorname{supp} A \subseteq G$ and write $\operatorname{wt}(A) = |\operatorname{supp} A|$ for its *weight*, the number of monomials in it. For $A \in R$ let L_A be the $N \times N$ matrix over $\mathbb{F}_2$ of multiplication by A in the basis G,

$$(L_A)_{g,h} = [\, g - h \in \operatorname{supp} A \,],$$

so that $L_A L_B = L_{AB}$. Following Galimova [1, §3], the *bicycle code* of a pair $(A, B) \in R^2$ is the CSS code on $n = 2N$ qubits with check matrices

$$H_X = (L_A \mid L_B), \qquad H_Z = (L_B^{\mathsf{T}} \mid L_A^{\mathsf{T}}), \qquad k = n - \operatorname{rank} H_X - \operatorname{rank} H_Z, \tag{1}$$

all ranks taken over $\mathbb{F}_2$. Orthogonality is automatic: $H_X H_Z^{\mathsf{T}} = L_A L_B + L_B L_A = 0$ because R is commutative. For G cyclic these are the generalized bicycle codes of Kovalev and Pryadko [3], studied further by Panteleev and Kalachev [2]; they are the abelian case of the two-block group algebra codes studied by Lin and Pryadko [5]; for $G = \mathbb{Z}_\ell \times \mathbb{Z}_m$ they are the bivariate bicycle codes, the family of the $[[72, 12, 6]]$ and $[[144, 12, 12]]$ codes of Bravyi et al. [8], and the case $G = \mathbb{Z}_{\ell_1} \times \mathbb{Z}_{\ell_2} \times \mathbb{Z}_{\ell_3}$ with $\operatorname{wt}(A) = \operatorname{wt}(B) = 3$ is the trivariate case studied in [1]. The quantity k is the number of logical qubits. We write $\exp G$ for the exponent of G, which for $G = \prod_i \mathbb{Z}_{\ell_i}$ is $\operatorname{lcm}(\ell_1, \ell_2, \dots)$.

The question. The source of the problem ran an empirical survey and published one sentence about it. Galimova [1, §4] writes, verbatim (the emphasis in the last sentence is ours):

> In a survey of over 170 tori, we observe empirically that $k = 6$ with weight-3 polynomials occurs only when $7 \mid \operatorname{lcm}(\ell_1, \ell_2, \ell_3)$. A partial algebraic explanation is as follows. Let

> $\mathrm{ord}_2(m)$ denote the multiplicative order of 2 modulo m …. Since $\mathrm{ord}_2(7) = 3$, the polynomial $x^7 - 1$ factors over $\mathbb{F}_2$ as $(x-1)(x^3+x+1)(x^3+x^2+1)$. This factorization gives three nontrivial irreducible $\mathbb{F}_2[\mathbb{Z}_7]$-submodules (of dimensions 1, 3, and 3). These three submodules provide enough independent structure for two weight-3 polynomials to achieve a six-dimensional kernel intersection. Since $\mathrm{ord}_2(p) = 3$ implies $p \mid 2^3 - 1 = 7$, the prime $p = 7$ is the only one with this property. **What remains unproven is whether other algebraic mechanisms (involving primes p with $\mathrm{ord}_2(p) \neq 3$) can also yield $k = 6$.**

No per-torus data accompanies the sentence, and no proof.

What is settled here. The missing step is the parity of the weight, and it costs one line. Write $\varepsilon\colon R \to \mathbb{F}_2$ for the augmentation, $\varepsilon(A) = \mathrm{wt}(A) \bmod 2$, and $Q = R/(A, B)$. The dimension formula of [2] — recalled, and cited rather than claimed, in §2 — gives $k = 2\dim_{\mathbb{F}_2} Q$. If A has odd weight then $\varepsilon(A) = 1$, and this forbids every $\mathbb{F}_2$-algebra homomorphism $Q \to \mathbb{F}_2$; a commutative unital $\mathbb{F}_2$-algebra admitting no such homomorphism is never 1-dimensional, is $\mathbb{F}_4$ if it is 2-dimensional and $\mathbb{F}_8$ if it is 3-dimensional (Proposition 3.2); and the images of G span Q, so one of them has multiplicative order 3 resp. 7.

Theorem (Theorem 4.1)**.** *Let G be a finite abelian group and $A, B \in \mathbb{F}_2[G]$ with $\mathrm{wt}(A)$ odd. Then the bicycle code* (1) *satisfies*

$$k \neq 2; \qquad k = 4 \implies 3 \mid \exp G; \qquad k = 6 \implies 7 \mid \exp G.$$

The last implication is the sentence quoted above, for every finite abelian G and every odd weight rather than for weight-3 pairs on a three-factor torus; the first two are corollaries the source does not state, and the first of those has been observed elsewhere without proof (see (iii) below). Because the ideal (A, B) is symmetric in its two generators, it is enough that *one* of A, B have odd weight. Nothing in the hypothesis constrains $|G|$ modulo 2, and this is the point of the route: it avoids the semisimple decomposition of $\mathbb{F}_2[G]$ entirely, and with it the distinction between odd and even $|G|$ on which the published machinery stops (see below).

For cyclic G the same three conclusions are reached along a second and independent route, directly over the polynomial form of the dimension formula, and that route is machine-checked for every ℓ at once (Theorem 5.1): a divisor g of $X^\ell - 1$ over $\mathbb{F}_2$ with $g(1) \neq 0$ never has degree 1, has degree 2 only if $3 \mid \ell$, and has degree 3 only if $7 \mid \ell$.

Finally, §6 reports an exhaustive weight-3 census over 30 presentations of abelian groups of order at most 56. It confirms the three implications where it looks, and it shows that neither divisibility implication reverses (Theorem 6.2): seven-divisibility is necessary for $k = 6$ and *not* sufficient — $\mathbb{Z}_2^3 \times \mathbb{Z}_7$ attains $12, 24, 48$ and never 6, while $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_7$ and $\mathbb{Z}_8 \times \mathbb{Z}_7$, of the same order 56 and also seven-divisible, do attain it — and $\mathbb{Z}_2^2 \times \mathbb{Z}_6$ is three-divisible with no $k = 4$. The census also carries a sharper statement than the three named values: every attained k lies in the set the odd-weight mechanism predicts from the 2-cyclotomic class degrees of the group alone, with no code computation in it.

Relation to previous work. Four things in the literature bear directly on this, and we are explicit about each.

(i) The dimension formula is published, and is cited here, never claimed. Panteleev and Kalachev [2, Prop. 1] prove that the generalized bicycle $[[2\ell, k]]$ code defined by $a(x), b(x) \in \mathbb{F}_2[x]/(x^\ell - 1)$ has $k = 2\deg g(x)$ with $g(x) = \gcd(a(x), b(x), x^\ell - 1)$; their own footnote credits a more complex form of the same to Kovalev and Pryadko [3, Thm. 2], who give, for the same pair of check matrices and in the notation used here, $k = 2\deg p + 2\deg r - 2\ell$ with $p = \gcd(a, x^\ell - 1)$ and $r = \gcd\big((x^\ell - 1)b/p,\ x^\ell - 1\big)$. The abelian form $k = 2\dim_{\mathbb{F}_2} \mathbb{F}_2[G]/(A, B)$ that we use is their argument plus one sentence about the antipode (§2); we do not take even that on trust, and Proposition 2.2 records what was verified instead.

(ii) The decomposition mechanism is published for G of odd order, and its authors leave the even case open. Eberhardt and Steffan [4, Prop. 4.3] prove that for ℓ and m odd the ring $R = \mathbb{F}_2[\mathbb{Z}_\ell \times \mathbb{Z}_m]$ is a direct sum of fields, described there through the quantity $n(d) = \varphi(d)/\,\mathrm{ord}_2(d)$ attached to a divisor

d of ℓ or of m, and [4, Cor. 4.4] that the quotient $R/(c,d)$ is then a product of finite fields $\mathbb{F}_{2^{n_i}}$. Of the even case they write (the ellipsis spans the rest of that sentence and the intervening text; the second sentence quoted opens a later remark of the same subsection): "The situation is more difficult ℓ or m is even. In this case, the ring R is non-reduced and the code $\mathrm{Code}(c,d)$ is not pure or principal in general … So, the even case reduces to the odd case and the 'nilpotent' case $\mathbb{F}_2[\underline{x}]/(\underline{x}^{k''})$. We leave the nilpotent case to the interested reader." This is exactly where the problem lives: all three of the $k = 6$ codes published in [1] sit on groups of *even* order, namely $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_7$, $\mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_7$ and $\mathbb{Z}_2 \times \mathbb{Z}_7 \times \mathbb{Z}_7$. Theorem 4.1 covers them because it never decomposes the ring: the structure-theoretic work is done instead by the finite enumeration of Proposition 3.2, which is insensitive to the parity of $|G|$. Eberhardt and Steffan draw no conclusion about which values k can take; what [1] says about that is the empirical sentence quoted above, and it is not proved there.

(iii) The impossibility of $k = 2$ has been observed, and not proved. Lin and Pryadko report, in the caption of [5, Fig. 3]: "We have not found any abelian-group codes with these weights and $k = 2$", the weights in question being $W_a = 3$ and W_b as indicated in that figure. The same paper contains the even-weight half of the augmentation observation, again verbatim: "for *even-even* codes, with both W_a and W_b even, rows and columns of the matrices … have even numbers of elements … this guarantees that the rows of the matrices A, B, and thus of the stabilizer generator matrices H_X, H_Z add to zero … we get non-trivial codes with $k \geq 2$. In comparison, with one or both weights odd, there are many trivial codes with $k = 0$." So the $k \neq 2$ half of Theorem 4.1 is an empirical observation in the literature; what is new is the proof, and the fact that it holds for every odd weight and every finite abelian G. We have found the implication $k = 4 \Rightarrow 3 \mid \exp G$ nowhere. What "nowhere" rests on: a full-text search of a local arXiv mirror (367 shards, 85 GB) turned up 140 papers that mention bicycle codes, of which none mentions an augmentation ideal or map, one mentions cyclotomic cosets (an unrelated bibliography line), eight mention odd weight — all read, none about the dimension of a bicycle code — and the only relevant hits on ord_2 or a semisimple group algebra are [4] and [1] themselves. OpenAlex reported no citing works for [1]; a positive control run against the same endpoint returned 11. A second citation index was rate-limited on both the query and the control, so it is recorded as unavailable rather than as zero.

(iv) One published identity that is not the one used here. Liang, Liu, Song and Chen [6] prove a dimension theorem for generalized toric codes on twisted tori of the shape

$$k_{\max} = 2\dim\bigl(\mathbb{Z}_2[x, y, x^{-1}, y^{-1}]/\langle f, g\rangle\bigr).$$

That quotient is taken over the *infinite* Laurent ring and the statement is an upper bound — the paper itself notes that "The ground state degeneracy could depend on the torus length" — so it is not the finite-group identity $k = 2\dim_{\mathbb{F}_2} \mathbb{F}_2[G]/(A,B)$ and we do not use it. We record this because the two are easy to conflate.

2. Preliminaries

Augmentation and the quotient algebra. The *augmentation* $\varepsilon\colon R \to \mathbb{F}_2$ is the $\mathbb{F}_2$-algebra homomorphism sending every $g \in G$ to 1; on a group-algebra element it returns the weight modulo 2. Write $I = (A,B) \trianglelefteq R$ for the ideal generated by the pair and $Q = R/I$ for the quotient, a commutative unital $\mathbb{F}_2$-algebra of finite dimension.

Proposition 2.1 (the dimension formula; [2, Prop. 1] for cyclic G)**.** *For every finite abelian G and $A, B \in R$ the code* (1) *has $k = 2\dim_{\mathbb{F}_2} Q$. For $G = \mathbb{Z}_\ell$ and a, b the polynomials of A, B this is* [2, Prop. 1]*, namely $k = 2\deg\gcd(a, b, x^\ell - 1)$.*

The argument for general abelian G is that of [2] with one extra sentence, and we give it because everything below is stated through Q. The column space of H_X is $\{Au + Bv : u, v \in R\} = I$, so $\operatorname{rank} H_X = \dim_{\mathbb{F}_2} I = N - \dim_{\mathbb{F}_2} Q$. The antipode $\sigma\colon g \mapsto -g$ is a ring automorphism of R — here G is abelian — and $(L_A^{\mathsf{T}})_{g,h} = (L_A)_{h,g} = [\,h - g \in \operatorname{supp} A\,] = (L_{\sigma A})_{g,h}$, so the column space of H_Z is $\sigma(I)$, of the same dimension as I. Hence $k = 2N - 2(N - \dim_{\mathbb{F}_2} Q) = 2\dim_{\mathbb{F}_2} Q$. The cyclic case is

published mathematics and is cited, not claimed; the extension is not assumed either, and the following proposition records what was checked in its place.

Proposition 2.2 (the model, verified rather than assumed)**.** *Let $\mathcal{N}(G)$ denote the set of pairs (A, B) of weight-3 elements of $\mathbb{F}_2[G]$ with $0 \in \operatorname{supp} A$ and $0 \in \operatorname{supp} B$. Then:*

(i) *the literal quantity $2N - \operatorname{rank} H_X - \operatorname{rank} H_Z$ of (1) equals $2 \dim_{\mathbb{F}_2} Q$ on every pair of $\mathcal{N}(G)$ for the eight groups $\mathbb{Z}_7$, $\mathbb{Z}_9$, $\mathbb{Z}_{21}$, $\mathbb{Z}_2 \times \mathbb{Z}_7$, $\mathbb{Z}_2^2 \times \mathbb{Z}_3$, $\mathbb{Z}_3 \times \mathbb{Z}_5$, $\mathbb{Z}_2 \times \mathbb{Z}_3^2$ and $\mathbb{Z}_2^2 \times \mathbb{Z}_7$ — that is, respectively, on $225 + 784 + 36100 + 6084 + 3025 + 8281 + 18496 + 123201 = 196\,196$ pairs;*

(ii) *$\operatorname{rank} H_X = \operatorname{rank} H_Z$ on every pair of $\mathcal{N}(G)$ for $\mathbb{Z}_7$, $\mathbb{Z}_9$, $\mathbb{Z}_2^2 \times \mathbb{Z}_3$ and $\mathbb{Z}_3 \times \mathbb{Z}_5$, that is on $12\,315$ pairs;*

(iii) *$H_X H_Z^{\mathsf{T}} = 0$ entrywise on all eight codes of Proposition 2.4;*

(iv) *restricting to $\mathcal{N}(G)$ loses nothing: the set of attained values of k over $\mathcal{N}(G)$ equals the set attained over* all *pairs of weight-3 elements, for $\mathbb{Z}_7$, $\mathbb{Z}_9$, $\mathbb{Z}_2 \times \mathbb{Z}_7$, $\mathbb{Z}_2^2 \times \mathbb{Z}_3$ and $\mathbb{Z}_3 \times \mathbb{Z}_5$, comparing $396\,202$ unnormalised pairs against their normalised counterparts.*

Remark 2.3. Part (iv) is also immediate: translating A by $g \in G$ multiplies it by the unit g of R, so the ideal (A, B) and therefore k are unchanged, and every weight-3 subset of G is a translate of exactly one containing 0. The census of §6 runs over $\mathcal{N}(G)$ for that reason, and (iv) is the check that the reduction was implemented as intended rather than an appeal to it.

Proposition 2.4 (the source's own table, recomputed)**.** *Each of the eight codes tabulated in* [1, Table 1] *— the two bivariate reference codes $[[72, 12, 6]]$ on 6×6 and $[[144, 12, 12]]$ on 12×6, which that table credits to Bravyi et al.* [8]*, the three weight-3 codes $[[84, 6, 10]]$, $[[140, 6, 14]]$ and $[[196, 6, 12]]$ on $2 \times 3 \times 7$, $2 \times 5 \times 7$ and $2 \times 7 \times 7$, the code $[[54, 8, 6]]$ on $3 \times 3 \times 3$, and the two self-dual even-weight codes $[[54, 14, 5]]$ on $3 \times 3 \times 3$ and $[[128, 20, 8]]$ on $4 \times 4 \times 4$ — reproduces its printed value of k, namely $12, 12, 6, 6, 6, 8, 14, 20$, when k is recomputed from (1) rather than read off the table; and $\operatorname{rank} H_X = \operatorname{rank} H_Z$ on every one of the eight, the common values being $30, 66, 39, 67, 95, 23, 20, 54$.*

Proof sketch. Both propositions are finite evaluations of the definitions in (1): group elements are mixed-radix indices, L_A and L_B are built as literal bitmask matrices, and the ranks are computed by Gaussian elimination over $\mathbb{F}_2$; $\dim_{\mathbb{F}_2} Q$ is computed independently, as N minus the dimension of the span of the two G-orbits $\{g + \operatorname{supp} A\}$ and $\{g + \operatorname{supp} B\}$. The two quantities are never identified in the code that computes them, which is what makes (i) a test. The monomial-to-index convention used in Proposition 2.4 was not guessed: the source prints two self-dual rows with $B = A^{\mathsf{T}}$ explicitly ($1 + x + y + z$ against $1 + x^2 + y^2 + z^2$ on $\mathbb{Z}_3^3$), which fixes the convention, and it then reproduces all eight rows. □

3. Commutative $\mathbb{F}_2$-algebras with no $\mathbb{F}_2$-point

Definition 3.1. An *$\mathbb{F}_2$-point* of a commutative unital $\mathbb{F}_2$-algebra Q is an $\mathbb{F}_2$-algebra homomorphism $Q \to \mathbb{F}_2$. We call Q *pointless* if it has none.

A commutative unital $\mathbb{F}_2$-algebra of dimension d together with a chosen basis $e_0 = 1, e_1, \ldots, e_{d-1}$ is exactly a symmetric bilinear multiplication on $\mathbb{F}_2^d$ for which e_0 is a unit and which is associative; it is determined by the $d(d-1)/2$ products $e_i e_j \in \mathbb{F}_2^d$ with $1 \le i \le j \le d-1$, so there are $2^{d \cdot d(d-1)/2}$ candidate tables in dimension d — 1, 4 and 512 for $d = 1, 2, 3$.

Proposition 3.2. *Of those candidate tables, exactly 1, 4 and 64 are associative, hence are $\mathbb{F}_2$-algebras, in dimensions 1, 2 and 3. Of these, exactly 0, 1 and 8 are pointless. In the pointless one of dimension 2, every element other than 0 and 1 has multiplicative order exactly 3; in each of the eight pointless ones of dimension 3, every element other than 0 and 1 has multiplicative order exactly 7.*

Proof sketch. Exhaustive enumeration of the $1 + 4 + 512$ tables. Unitality, commutativity and associativity are tested on all element pairs and triples — 2^d elements, so 8, 64 and 512 triples — and not merely on basis vectors; an $\mathbb{F}_2$-point is an $\mathbb{F}_2$-linear functional φ with $\varphi(1) = 1$ and $\varphi(xy) = \varphi(x)\varphi(y)$, and all 2^d functionals are tried; multiplicative orders are computed for all 2^d elements. The count 8

in dimension 3 is 24/3: the 24 ordered bases $(1, u, v)$ of $\mathbb{F}_8$ fall into 8 orbits under its Galois group of order 3. □

Corollary 3.3. *A pointless commutative unital $\mathbb{F}_2$-algebra is not 1-dimensional; if it is 2-dimensional it is $\mathbb{F}_4$, and if it is 3-dimensional it is $\mathbb{F}_8$.*

Proof. Immediate from Proposition 3.2: in dimension 2 resp. 3 every nonzero element x satisfies $x^3 = 1$ resp. $x^7 = 1$, hence $x \cdot x^2 = 1$ resp. $x \cdot x^6 = 1$ is invertible, so the algebra is a field of 4 resp. 8 elements. □

Remark 3.4 (the hypothesis is doing work). Neither half of Proposition 3.2 survives weakening. Dropping pointlessness destroys the conclusion: it is false that every 3-dimensional commutative unital $\mathbb{F}_2$-algebra has all its elements other than $0, 1$ of order 7, as $\mathbb{F}_2^3$ itself shows and as the enumeration confirms. And the dimension-2 conclusion does not carry over to dimension 3: it is false that the eight pointless 3-dimensional algebras have all their elements other than $0, 1$ of order 3. Both statements are part of the verified enumeration.

4. The theorem for abelian G

Theorem 4.1. *Let G be a finite abelian group and $A, B \in \mathbb{F}_2[G]$ with $\mathrm{wt}(A)$ odd. Then the bicycle code (1) satisfies*

$$\textit{(i) } k \neq 2; \qquad \textit{(ii) } k = 4 \implies 3 \mid \exp G; \qquad \textit{(iii) } k = 6 \implies 7 \mid \exp G.$$

Since $(A, B) = (B, A)$ as ideals, the hypothesis may be weakened to: at least one of A, B has odd weight.

Proof. Write $I = (A, B)$ and $Q = R/I$; by Proposition 2.1, $\dim_{\mathbb{F}_2} Q = k/2$, so the three conclusions are the assertions that $\dim_{\mathbb{F}_2} Q$ is not 1, that $\dim_{\mathbb{F}_2} Q = 2$ forces $3 \mid \exp G$, and that $\dim_{\mathbb{F}_2} Q = 3$ forces $7 \mid \exp G$.

Step 1: Q is pointless. Suppose $\varphi\colon Q \to \mathbb{F}_2$ is an $\mathbb{F}_2$-algebra homomorphism. Composing with the surjection $R \twoheadrightarrow Q$ gives an $\mathbb{F}_2$-algebra homomorphism $\psi\colon \mathbb{F}_2[G] \to \mathbb{F}_2$. Its restriction to G takes values in $\mathbb{F}_2^\times = \{1\}$, since every $g \in G$ is a unit of R of finite order, so ψ agrees with the augmentation ε on a basis and hence $\psi = \varepsilon$. But $A \in I$ gives $\psi(A) = 0$, while $\varepsilon(A) = \mathrm{wt}(A) \bmod 2 = 1$ — a contradiction.

Step 2: the possible shapes of Q. By Proposition 3.2 there is no pointless algebra of dimension 1, so $\dim_{\mathbb{F}_2} Q \neq 1$, which is (i); and if $\dim_{\mathbb{F}_2} Q$ is 2 or 3 then, again by that proposition, every element of Q other than 0 and 1 has multiplicative order exactly 3 resp. 7 (equivalently, by Corollary 3.3, Q is $\mathbb{F}_4$ resp. $\mathbb{F}_8$).

Step 3: back to G. Suppose $\dim_{\mathbb{F}_2} Q \in \{2, 3\}$. The images of G span Q over $\mathbb{F}_2$, because $R \twoheadrightarrow Q$ and R is spanned by G. If every $g \in G$ had image 1, then Q would be spanned by 1 and $\dim_{\mathbb{F}_2} Q = 1$; so some $g \in G$ has image $q \neq 1$, and $q \neq 0$ because g is a unit of R. By Step 2 the multiplicative order of q is 3 resp. 7. Since $q^{\mathrm{ord}(g)} = 1$, that order divides $\mathrm{ord}(g)$, which divides $\exp G$. This is (ii) resp. (iii). □

Remark 4.2 (what the proof does not use). No Artin–Wedderburn decomposition, no Hensel lifting, no semisimplicity, and no hypothesis on $|G|$ modulo 2. All of the structure theory is discharged by the finite enumeration of Proposition 3.2, and that is what lets the theorem reach the even-order groups on which [4] stops and on which all of the source's $k = 6$ codes live.

Remark 4.3 (verification status of Theorem 4.1). Of the ingredients of the proof, Proposition 3.2 — which is all that Step 2 consumes — is machine-checked, as is the cyclic instance of the conclusion, Theorem 5.1, along an independent route. Step 1 and Step 3, three lines each, the one-line Corollary 3.3, and the abelian half of Proposition 2.1 are ordinary mathematics, written out above and not part of the formal development; the obstacle is a coordinate basis for $\mathbb{F}_2[G]/(A, B)$ over a general finite abelian G in the library used, not any difficulty in the argument. §7 says exactly what is machine-checked and what is not.

Corollary 4.4. *Let $G = \mathbb{Z}_{\ell_1} \times \mathbb{Z}_{\ell_2} \times \mathbb{Z}_{\ell_3}$ and let $A, B \in \mathbb{F}_2[G]$ be weight-3 polynomials. If the resulting bicycle code has $k = 6$ then $7 \mid \mathrm{lcm}(\ell_1, \ell_2, \ell_3)$.*

Remark 4.5 (the odd-weight hypothesis cannot be dropped). Both failures are witnessed by the source's own published data. On the 2-group $\mathbb{Z}_4^3$ every weight-3 pair gives $k = 0$ — an odd-weight element has augmentation 1 and is therefore a unit in the local ring $\mathbb{F}_2[\mathbb{Z}_4^3]$ — while the even-weight self-dual code $[[128, 20, 8]]$ of [1, Table 1] on that same group has $k = 20$. On $\mathbb{Z}_3^3$ every weight-3 pair gives $4 \mid k$, that is an even $\dim_{\mathbb{F}_2} Q$, while the even-weight code $[[54, 14, 5]]$ of [1, Table 1] there has $k = 14$, an odd dimension 7. Both contrasts are verified.

5. The cyclic case, for every ℓ at once

For $G = \mathbb{Z}_\ell$ the dimension formula takes the polynomial form of [2, Prop. 1], and the three conclusions of Theorem 4.1 can be read off the possible degrees of $g = \gcd(a, b, X^\ell - 1)$ without any algebra enumeration. This is the route that is fully machine-checked, and it is proved for all ℓ simultaneously.

Theorem 5.1. *Let $\ell > 0$ and let $g \in \mathbb{F}_2[X]$ divide $X^\ell - 1$ with $g(1) \neq 0$. Then*

$$\deg g \neq 1; \qquad \deg g = 2 \implies 3 \mid \ell; \qquad \deg g = 3 \implies 7 \mid \ell.$$

Consequently, for $a, b \in \mathbb{F}_2[X]$ with $a(1) \neq 0$ — that is, for a cyclic bicycle code on $\mathbb{Z}_\ell$ whose A has odd weight — the polynomial $g = \gcd\big(\gcd(a, b), X^\ell - 1\big)$ satisfies the same three statements, so through $k = 2 \deg g$ the code has $k \neq 2$, has $k = 4$ only if $3 \mid \ell$, and has $k = 6$ only if $7 \mid \ell$.

Proof sketch. Two elementary reductions come first. A divisor of $X^\ell - 1$ has nonzero constant term, since $X \mid X^\ell - 1$ is false for $\ell > 0$; and if A has odd weight then $a(1) = 1$, so $g \mid a$ forces $g(1) \neq 0$ — this is the step the partial explanation in [1] is missing, and it is the entire content of "odd".

Now let g have $g(0) \neq 0$ and $g(1) \neq 0$. Extracting the four low coefficients and case-splitting on $\mathbb{F}_2$: no such g has degree 1, because $X + 1$ is the only monic degree-1 polynomial over $\mathbb{F}_2$ with nonzero constant term and it vanishes at 1; in degree 2 the only candidate is $X^2 + X + 1$; in degree 3 the only candidates are $X^3 + X + 1$ and $X^3 + X^2 + 1$. Explicit cofactors give $X^2 + X + 1 \mid X^3 - 1$ and $X^3 + X + 1,\ X^3 + X^2 + 1 \mid X^7 - 1$. The bridge from those divisibilities to ℓ is the descent

$$g \mid X^\ell - 1 \ \text{ and } \ g \mid X^m - 1 \quad \implies \quad g \mid X^{\gcd(\ell, m)} - 1,$$

proved over an arbitrary commutative ring from $X^r - 1 = (X^{\ell q + r} - 1) - X^r(X^{\ell q} - 1)$ together with $X^\ell - 1 \mid X^{\ell q} - 1$. If $\deg g = 3$ and $7 \nmid \ell$ then $\gcd(\ell, 7) = 1$ and the descent gives $g \mid X - 1$, contradicting $\deg g = 3$; the degree-2 case is the same with 3 in place of 7. The whole argument is formal and finite-case-analytic; it involves no search. □

Remark 5.2 (controls). The conclusion is not vacuous: $X^3 + X + 1$ divides $X^7 - 1$, does not vanish at 1, and has degree 3, so the degree-3 case really occurs, on $\ell = 7$. And the hypothesis $g(1) \neq 0$ cannot be dropped: $X + 1$ divides $X^\ell - 1$ for every ℓ, has degree 1, and vanishes at 1, so without it the degree-1 case is not excluded and nothing about ℓ follows. Both are verified.

6. The weight-3 census

The source reports a survey of "over 170 tori" and publishes no per-torus data. This section publishes data of that kind, exhaustively, for a list of our own choosing: 30 presentations of finite abelian groups of order at most 56. It is also what shows the two divisibility implications of Theorem 4.1 not to reverse. For each group all pairs (A, B) of weight-3 elements with $0 \in \operatorname{supp} A$, $0 \in \operatorname{supp} B$ are swept (Remark 2.3) and the exact set of attained values $k > 0$ is recorded. That is 9 959 476 normalised pairs, visited as 4 985 596 unordered ones because $\dim_{\mathbb{F}_2} Q$ is symmetric in A and B, and they stand for 2 770 442 265 unnormalised pairs.

Theorem 6.1 (the census)**.** *Table 1 is exhaustive: for each of its* 30 *rows, the listed set is exactly the set of values $k > 0$ attained by a pair of weight-*3 *elements of $\mathbb{F}_2[G]$. The exponent column is computed as* lcm *of the listed factor orders rather than transcribed.*

G	N	$\exp G$	$7 \mid \exp G$	attained $k > 0$
$\mathbb{Z}_2^3$	8	2		—
$\mathbb{Z}_2^2 \times \mathbb{Z}_4$	16	4		—
$\mathbb{Z}_2 \times \mathbb{Z}_4^2$	32	4		—
$\mathbb{Z}_2^2 \times \mathbb{Z}_5$	20	10		—
$\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_5$	40	20		—
$\mathbb{Z}_2^2 \times \mathbb{Z}_3$	12	6		$4, 8, 16$
$\mathbb{Z}_2^2 \times \mathbb{Z}_6$	24	6		$8, 16, 32$
$\mathbb{Z}_2 \times \mathbb{Z}_3^2$	18	6		$4, 8, 12, 16, 24$
$\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_4$	24	12		$4, 8, 16, 32$
$\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$	30	30		$4, 8, 16, 20, 40$
$\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_6$	36	6		$4, 8, 12, 16, 24, 32, 48$
$\mathbb{Z}_3^3$	27	3		$4, 8, 12, 24, 36$
$\mathbb{Z}_3^2 \times \mathbb{Z}_4$	36	12		$4, 8, 12, 16, 24, 32, 48$
$\mathbb{Z}_7$	7	7	•	6
$\mathbb{Z}_2 \times \mathbb{Z}_7$	14	14	•	$6, 12$
$\mathbb{Z}_{14}$	14	14	•	$6, 12$
$\mathbb{Z}_3 \times \mathbb{Z}_7$	21	21	•	$4, 6, 10, 12, 18, 28$
$\mathbb{Z}_{21}$	21	21	•	$4, 6, 10, 12, 18, 28$
$\mathbb{Z}_5 \times \mathbb{Z}_7$	35	35	•	$6, 30$
$\mathbb{Z}_2^2 \times \mathbb{Z}_7$	28	14	•	$6, 12, 24$
$\mathbb{Z}_9$	9	9		$4, 12$
$\mathbb{Z}_{11}$	11	11		—
$\mathbb{Z}_{13}$	13	13		—
$\mathbb{Z}_3 \times \mathbb{Z}_5$	15	15		$4, 8, 20$
$\mathbb{Z}_5^2$	25	5		—
$\mathbb{Z}_4 \times \mathbb{Z}_7$	28	28	•	$6, 12, 24$
$\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_7$	42	42	•	$4, 6, 8, 10, 12, 18, 20, 24, 28, 36, 56$
$\mathbb{Z}_2^3 \times \mathbb{Z}_7$	56	14	•	$12, 24, 48$
$\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_7$	56	28	•	$6, 12, 24, 48$
$\mathbb{Z}_8 \times \mathbb{Z}_7$	56	56	•	$6, 12, 24, 48$

TABLE 1. The exhaustive weight-3 census. Two pairs of rows present the same group twice ($\mathbb{Z}_{14}$ with $\mathbb{Z}_2 \times \mathbb{Z}_7$, and $\mathbb{Z}_{21}$ with $\mathbb{Z}_3 \times \mathbb{Z}_7$), so the 30 rows are 28 distinct groups; the duplicated rows agree, which is a control on the mixed-radix indexing of G. Row $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_7$ is the group of the source's own $[[84, 6, 10]]$ code.

What the mechanism predicts. Before reading the table, it is worth writing down what the odd-weight argument allows, from the group alone. Split $G = G_2 \times G'$ into its Sylow 2-subgroup and its odd part. Since $|G'|$ is odd, the characters of G' over an algebraic closure of $\mathbb{F}_2$ fall into orbits under $\chi \mapsto \chi^2$ — the 2-*cyclotomic classes* — and the orbit of a character of order m has size $\mathrm{ord}_2(m)$. Let $D(G)$ be the multiset of orbit sizes, one entry per *nontrivial* orbit; every $d \in D(G)$ satisfies $d \geq 2$, because $\mathrm{ord}_2(m) = 1$ forces $m \mid 1$. Put

$$P(G) = \Big\{ \textstyle\sum_{d \in D(G)} d\, m_d \ : \ 0 \leq m_d \leq |G_2| \Big\},$$

one multiplier per class, counted with multiplicity. The motivation is the classical splitting $\mathbb{F}_2[G'] \cong \prod_j \mathbb{F}_{2^{d_j}}$, whence $\mathbb{F}_2[G] \cong \prod_j \mathbb{F}_{2^{d_j}}[G_2]$ with each factor local of residue field $\mathbb{F}_{2^{d_j}}$ and of $\mathbb{F}_{2^{d_j}}$-dimension $|G_2|$: each factor of the quotient is an $\mathbb{F}_{2^{d_j}}$-space of dimension at most $|G_2|$, and odd weight makes the image of A in the trivial-class factor a unit, deleting the class of degree 1. We use $P(G)$ only as a prediction of which $k = 2\dim_{\mathbb{F}_2} Q$ are *allowed*; no statement below is proved from it, and $P(G)$ says nothing about which values are *attained* by weight-3 pairs.

Theorem 6.2 (the census against the three implications)**.** *On the* 30 *rows of Table 1:*

(i) *no row attains $k = 2$;*

(ii) *$k = 6$ is attained only on rows with $7 \mid \exp G$, and not on all of them: twelve rows are seven-divisible and eleven attain $k = 6$. The exception is $\mathbb{Z}_2^3 \times \mathbb{Z}_7$, which attains $12, 24, 48$; the groups $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_7$ and $\mathbb{Z}_8 \times \mathbb{Z}_7$ have the same order 56, are also seven-divisible, and do attain $k = 6$;*

(iii) *$k = 4$ is attained only on rows with $3 \mid \exp G$, and again not on all of them: exactly one row, $\mathbb{Z}_2^2 \times \mathbb{Z}_6$, is three-divisible and attains no $k = 4$;*

(iv) *every attained value of k lies in $2P(G)$, on every row;*

(v) *and, computed from the group alone, $6 \in 2P(G)$ if and only if $7 \mid \exp G$, $4 \in 2P(G)$ if and only if $3 \mid \exp G$, and $2 \notin 2P(G)$ on every row.*

Proof sketch. Parts (i)–(iii) are read off Table 1, whose content is Theorem 6.1; the reading itself is a finite check over the tabulated rows. The table is the expensive part: for each group, all normalised weight-3 pairs are enumerated and $\dim_{\mathbb{F}_2} Q$ is computed for each by row-reducing the two G-orbits, for a total of 9 959 476 pairs, visited as 4 985 596 unordered ones. Nothing is sampled and nothing is pruned except by the two exact reductions of Remark 2.3 and the symmetry of $\dim_{\mathbb{F}_2} Q$ in A and B. Parts (iv) and (v) are evaluations of $P(G)$ — the character orders of G', their 2-cyclotomic class sizes, and then all sums $\sum_d d\, m_d$ with $0 \le m_d \le |G_2|$ — and a containment test against the table; the computation of $P(G)$ never looks at a code. □

Remark 6.3 (why (v) is an equivalence and (ii), (iii) are not). The two halves of the theorem are different in kind, and the difference is the honest shape of the subject: the mechanism says which values of k are *allowed* by the group, the census which are *attained* by weight-3 pairs. Part (v) is in fact elementary and general, though we state it only where it is verified. Since every $d \in D(G)$ is at least 2, a representation $3 = \sum d\, m_d$ needs a single class of degree 3; and $\mathrm{ord}_2(m) = 3$ holds exactly when $m \mid 7$ and $m \neq 1$, that is $m = 7$, so $3 \in P(G)$ if and only if G has a character of order 7, i.e. $7 \mid \exp G$. The same argument with $\mathrm{ord}_2(m) = 2$, which holds exactly for $m = 3$, gives $2 \in P(G)$ if and only if $3 \mid \exp G$; and $1 \in P(G)$ is impossible. On $\mathbb{Z}_2^3 \times \mathbb{Z}_7$ the value 6 is therefore allowed and simply not reached by any weight-3 pair.

Remark 6.4 (controls on the census). The containment (iv) is strict on 27 of the 30 rows, so it must not be read as an equality; the census is not vacuous, 22 of the 30 rows attaining some $k > 0$; $k = 6$ really occurs, on $\mathbb{Z}_7$, where the attained set is exactly $\{6\}$; and it does not occur everywhere, $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$ attaining $4, 8, 16, 20, 40$ and no 6. All four are verified.

Remark 6.5 (data outside the formal development). The following computations were run outside the formal development and are reported as measurements; no statement above depends on them. Three further exhaustive weight-3 censuses: $\mathbb{Z}_7^2$ ($N = 49$) attains $\{6, 12, 18, 42\}$; $\mathbb{Z}_3^2 \times \mathbb{Z}_5$ ($N = 45$) attains $\{4, 8, 12, 16, 20, 24, 40, 60\}$; and the rank-4 group $\mathbb{Z}_2 \times \mathbb{Z}_3^3$ ($N = 54$), outside the three-factor setting of [1] altogether, attains $\{4, 8, 12, 16, 24, 36, 48, 72\}$. Five exhaustive weight-5 censuses, which no part of the source or of Table 1 touches: $\mathbb{Z}_7 \to \emptyset$, $\mathbb{Z}_9 \to \{4\}$, $\mathbb{Z}_2 \times \mathbb{Z}_7 \to \{6\}$, $\mathbb{Z}_2^2 \times \mathbb{Z}_3 \to \{4, 8, 12\}$ and $\mathbb{Z}_3 \times \mathbb{Z}_5 \to \{4, 8, 12, 16, 24\}$. And an adversarial sample: 10 740 random odd-weight pairs, of weights 3 and 5, on 92 abelian groups of order at most 60, each tested against all three conclusions of Theorem 4.1, with zero violations — no $k = 2$ anywhere, no $k = 4$ on a group with $3 \nmid \exp G$, no $k = 6$ on a group with $7 \nmid \exp G$. Every one of these sets lies inside its predicted set $2P(G)$.

Remark 6.6 (an example in the literature that is not a counterexample). Wang and Pryadko [7] exhibit the weight-3 pair $a = y^2 + xy + x^2y^2$, $b = 1 + x^2 + y^2$ and write "This polynomial pair gives a code family with $k = 6$, smaller than expected for $D = 2$ tiles." That is a planar tile code with open boundaries — "five qubits and three X generators must be dropped, which gives a code with parameters $[[45, 6, 3]]$", and 45 is odd, so it is not a bicycle code on a group. Read instead as a pair on $\mathbb{Z}_\ell \times \mathbb{Z}_m$, the same (a, b) was evaluated on all 100 groups with $3 \le \ell, m \le 12$ and never gives $k = 6$ without $7 \mid \mathrm{lcm}(\ell, m)$, in agreement with Theorem 4.1. (This last evaluation is outside the formal development.)

7. Verification

Formally verified in Lean 4 [9] are: Propositions 2.2, 2.4 and 3.2; Theorems 5.1, 6.1 and 6.2; and the controls of Remarks 3.4, 4.5, 5.2 and 6.4. Not formally verified, and written out above as ordinary mathematics, are: Proposition 2.1, which is [2, Prop. 1] for cyclic G and that paper's argument plus one

sentence about the antipode for abelian G — an extension that is nowhere assumed but tested instead, by Proposition 2.2; the one-line Corollary 3.3; Steps 1 and 3 of Theorem 4.1, with its Corollary 4.4; the elementary observation of Remark 6.3; and the measurements of Remarks 6.5 and 6.6, which are labelled as such where they occur and on which nothing else depends. Theorem 5.1 is proved over *Mathlib* [10] for all ℓ simultaneously and depends on no evaluation axiom: its only axioms are the three standard ones (`propext`, `Classical.choice`, `Quot.sound`). The census reading of Theorem 6.2(i)–(iii) is decided by the kernel itself, over the tabulated data, with no axioms at all. The remaining verified statements are finite evaluations carried out by Lean's compiled evaluator (`native_decide`), so each depends on `propext` together with one evaluation axiom, and that evaluator is the only trusted step there; the modules carrying those evaluations import no mathematical library, every object being a natural number or a list of them, so the check-matrix definition (1) is transcribed directly rather than through any criterion. There is no `sorry` anywhere in the development and it declares no axiom of its own. The two heaviest items are the 30-group census (937 seconds on a heavily loaded machine, split into three evaluations so that no single one carries the whole run) and the pairwise comparison of the two definitions of k in Proposition 2.2 (653 seconds); the algebra enumeration is 14 seconds and Theorem 5.1 is 8 seconds over *Mathlib*. An independently written program in another language reproduces the census and all eight values of Proposition 2.4. The repository is private; repository reference to be added at submission.

8. What is left open

When is $k = 6$ actually attained? Theorem 4.1 says $7 \mid \exp G$ is necessary; Table 1 says it is not sufficient. The three rows of order 56 are the smallest data set that constrains the missing condition: $\mathbb{Z}_2^3 \times \mathbb{Z}_7$, $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_7$ and $\mathbb{Z}_8 \times \mathbb{Z}_7$ are all seven-divisible, and only the last two carry a weight-3 code with $k = 6$. What separates them is the structure of the 2-part, that is the local ring $\mathbb{F}_8[G_2]$ and how small a quotient a weight-3 element can cut out of it — which is precisely the "nilpotent case" that [4] leaves to the interested reader. A sufficient condition for $k = 6$ is the question this paper inherits.

The next dimension. The same enumeration in dimension 4 would give the $k = 8$ line. The count is $2^{4\cdot 6} = 16\,777\,216$ candidate tables with $16^3 = 4096$ associativity triples each, about 7×10^{10} triples; we have not run it. What one expects from the prediction $P(G)$ is a disjunction rather than a single prime: a representation $4 = \sum d\, m_d$ with all $d \geq 2$ needs either a class of degree 4 — and $\mathrm{ord}_2(m) = 4$ holds exactly for $m \in \{5, 15\}$, so $5 \mid \exp G$ — or two contributions of degree 2, so that $3 \mid \exp G$. So the expected shape is: $k = 8$ forces $3 \mid \exp G$ or $5 \mid \exp G$. We state this as an expectation, not as a theorem.

Wider groups, and weights beyond 3. The census stops at $N = 56$; the natural next cells are $N = 63, 70, 72$ and, for the group of the source's own $[[196, 6, 12]]$ code, $\mathbb{Z}_2 \times \mathbb{Z}_7^2$ at $N = 98$, whose weight-3 sweep is about 1.1×10^7 normalised pairs and was priced rather than run. Nothing in Theorem 4.1 is about weight 3; only the census is. The five weight-5 censuses of Remark 6.5 are a first probe of that gap, and a systematic weight-5 census on the small groups would test how much of the predicted set $P(G)$ is attained at all.

References

[1] A. A. Galimova, *Independent Trivariate Bicycle Codes*, arXiv:2603.17703v1, announced 18 March 2026 (quant-ph primary, cs.IT cross-list). No journal version; v1 is the only version as of 30 August 2026. Section and table numbers above are those of the typeset v1: §3 is "Code construction", §4 is "Code instances", and the table of codes is Table 1.

[2] P. Panteleev and G. Kalachev, *Degenerate Quantum LDPC Codes With Good Finite Length Performance*, Quantum **5**, 585 (2021), `doi:10.22331/q-2021-11-22-585`; arXiv:1904.02703v3. Proposition 1 is the first proposition of the document, under an unsectioned counter; the number is that of the typeset v3.

[3] A. A. Kovalev and L. P. Pryadko, *Quantum Kronecker sum-product low-density parity-check codes with finite rate*, Phys. Rev. A **88**, 012311 (2013), `doi:10.1103/PhysRevA.88.012311`; arXiv:1212.6703v2, where the title reads *Quantum "hyperbicycle" low-density parity check codes with finite rate*. Theorem 2 is the number in the typeset v2; it is the theorem the footnote of [2] points to.

[4] J. N. Eberhardt and V. Steffan, *Logical Operators and Fold-Transversal Gates of Bivariate Bicycle Codes*, arXiv:2407.03973v1 (quant-ph primary, cs.IT cross-list); v1 is the only version as of 30 August 2026. Proposition 4.3 and Corollary 4.4 are the numbers in the typeset v1.

[5] H.-K. Lin and L. P. Pryadko, *Quantum two-block group algebra codes*, arXiv:2306.16400v1 (quant-ph primary, math-ph cross-list); published as Phys. Rev. A **109**, 022407 (2024), doi:10.1103/PhysRevA.109.022407. Figure 3 is the number in the typeset v1 of the e-print, which is what was read.

[6] Z. Liang, K. Liu, H. Song and Y.-A. Chen, *Generalized toric codes on twisted tori for quantum error correction*, PRX Quantum **6**, 020357 (2025), doi:10.1103/rmy6-9n89; arXiv:2503.03827v3.

[7] R. Wang and L. P. Pryadko, *Algebra of Bivariate-Bicycle Surface Codes*, arXiv:2606.08771v1 (quant-ph primary, cs.IT cross-list); v1 is the only version as of 30 August 2026. No journal version.

[8] S. Bravyi, A. W. Cross, J. M. Gambetta, D. Maslov, P. Rall and T. J. Yoder, *High-threshold and low-overhead fault-tolerant quantum memory*, Nature **627**, 778–782 (2024), doi:10.1038/s41586-024-07107-7; arXiv:2308.07915v2. This is the reference [1, Table 1] itself gives for its two bivariate reference codes.

[9] L. de Moura and S. Ullrich, *The Lean 4 theorem prover and programming language*, in: A. Platzer and G. Sutcliffe (eds.), Automated Deduction — CADE 28, Lecture Notes in Computer Science **12699**, Springer, Cham, 2021, pp. 625–635; doi:10.1007/978-3-030-79876-5_37.

[10] The mathlib Community, *The Lean mathematical library*, in: Certified Programs and Proofs (CPP 2020), ACM, 2020, pp. 367–381; doi:10.1145/3372885.3373824.