

# SMALL VERTEX-MINOR UNIVERSAL GRAPHS: AN ORDER-15 WITNESS AT $k = 5$ , THE EXACT VERTEX-MINOR DEFICIT OF AN EXTREMAL ORDER-14 GRAPH, AND THE FIRST VALUES OVER $\mathbb{F}_p$

KOREA SUPERINTELLIGENCE LABS

ABSTRACT. A graph  $G$  is  $k$ -vertex-minor universal if every graph on every  $k$  of its vertices is a vertex-minor of  $G$ . Let  $\nu(k)$  be the least order of such a graph; the first three values are  $\nu(2) = 3$ ,  $\nu(3) = 6$ ,  $\nu(4) = 10$ , and at  $k = 5$  the best published bound is  $\nu(5) \leq 17$ , from the Paley graph of order 17. We exhibit a 5-vertex-minor universal graph of order 15, so  $\nu(5) \leq 15$ , together with a covering family of 8880 explicit local-complementation words that certifies it over all 3075072 (subset, target) cells. We then analyse the extremal end of order 14. For the published extremal  $(14, 2^{14}, 6)$  self-dual additive  $GF(4)$  code with graph6 string `MAa_0KrD]U1V|r}~?`, we determine its vertex-minor deficit exactly, and unconditionally: 2050036 of the 2050048 cells are realised, by 7233 explicit words, and the remaining twelve are realised by no sequence of local complementations at all. All twelve missing targets are labellings of  $2K_2 \cup K_1$ , which is a local-complementation fixed point. The negative half rests on a blocking criterion, read off the graph-state code and proved here from scratch, which also shows that the Paley graph of order 13 and eight extremal order-13 candidates are not 5-vertex-minor universal.

The second half of the paper opens a new axis. Replacing graphs by symmetric zero-diagonal matrices over  $\mathbb{F}_p$  and local complementation by the two operations of Bahramgiri and Beigi, we define  $k$ -vertex-minor universality for qudit graph states and write  $\nu_p(k)$  for the corresponding minimal order. We prove  $\nu_p(2) = 3$  for every  $p$  with  $\mathbb{F}_p$  a domain, uniformly in  $p$  and with no computation; we prove  $\nu_3(3) = 6$  with the all-ones 6-cycle as witness,  $6 \leq \nu_3(4) \leq 10$  with the all-ones Petersen graph, and  $5 \leq \nu_5(3) \leq 6$ . The same 6-cycle is the  $k = 3$  witness at  $p = 2, 3, 5$  and the same Petersen graph the  $k = 4$  witness at  $p = 2, 3$ , which raises the question whether  $\nu_p(k)$  depends on  $p$  at all. Every theorem and proposition below is formally verified in Lean 4; the computations reported alongside them are flagged, where they occur, as lying outside that development.

## 1. INTRODUCTION

Let  $G = (V, E)$  be a finite simple graph and  $u \in V$ . *Local complementation at  $u$*  produces the graph

$$G \star u = G \triangle K_{N_G(u)},$$

obtained by complementing the subgraph induced on the neighbourhood of  $u$  and leaving every other adjacency, including those at  $u$ , alone. Two graphs on the same vertex set are *locally equivalent*, written  $G \equiv_{\text{LC}} G'$ , if one is carried to the other by a sequence of local complementations. A graph  $F$  with vertex set  $V' \subseteq V$  is a *vertex-minor* of  $G$  if it can be reached from  $G$  by a sequence of local complementations and vertex deletions; equivalently — and this is the form we use throughout — if there is a graph  $G' \equiv_{\text{LC}} G$  with  $G'[V'] = F$ , the deletions being performed last.

**Definition 1.1.**  $G$  is  *$k$ -vertex-minor universal* if every graph on every  $k$ -subset of  $V(G)$  is a vertex-minor of  $G$ . We write  $\nu(k)$  for the least order of a  $k$ -vertex-minor universal graph.

Throughout, graphs on a  $k$ -subset  $S$  are *labelled*:  $S$  is a fixed set of vertices of  $G$  and  $G'[S] = F$  is an equality of graphs on  $S$ , not an isomorphism. So a graph of order  $n$  is  $k$ -vertex-minor universal exactly when it realises all  $\binom{n}{k} 2^{\binom{k}{2}}$  cells  $(S, F)$ ,  $S$  a  $k$ -subset and  $F$  a labelled graph on  $S$ .

The notion comes from quantum information. If  $|G\rangle$  is the graph state of  $G$ , then  $F$  being a vertex-minor of  $G$  says exactly that the graph state  $|F\rangle$  can be induced on the qubits  $V'$  using local Clifford unitaries, local destructive Pauli measurements and classical communication; so  $k$ -vertex-minor universality says that *any*  $k$ -qubit stabilizer state can be produced on *any*  $k$  of the qubits by

those means. It strictly strengthens the  $k$ -pairability of Bravyi, Sharma, Szegedy and de Wolf [7]: a  $2k$ -vertex-minor universal graph is  $k$ -pairable. Claudet, Mhalla and Perdrix [11] showed that a  $k$ -vertex-minor universal graph must have  $\Omega(k^2)$  vertices, and Cautrès, Claudet, Mhalla, Perdrix, Savin and Thomassé [8] matched that order, exhibiting  $k$ -vertex-minor universal random bipartite graphs of order  $\Theta(k^2)$ ; Chapter 7 of Claudet’s thesis [10] develops that asymptotic result and, in a separate section, the small-order question we take up here.

**What is known about  $\nu$ .** The source [10] records three values and no more. Its evidence is explicitly numerical: the words used are “we observed” and “numerical analysis indicates”.

$$\nu(2) = 3 \ (K_3), \quad \nu(3) = 6 \ (C_6), \quad \nu(4) = 10.$$

The order-10 witnesses are the “wheel” graph of [7] — which is the Möbius ladder  $C_{10}(1, 5)$ , a 10-cycle together with its five long diagonals — and the Petersen graph; the lower half at  $k = 4$  is the thesis’s inference from the verbatim statement of [7] that no stabilizer state on fewer than ten qubits is 2-pairable by Pauli measurements. At  $k = 5$  the source prints no value. Its best bound is

$$(1) \quad \nu(5) \leq 17,$$

from the assertion that the Paley graph of order 17 is 5-vertex-minor universal. Since 3, 6, 10 are the triangular numbers  $\binom{k+1}{2}$ , the value 15 is the one the first three terms invite, and closing the gap between 15 and 17 is the natural first question.

Two necessary conditions from [10] organise every search. Write  $\delta_{\text{loc}}(G)$  for the minimum degree taken over the whole local equivalence class of  $G$ . Then

$$(2) \quad G \text{ is } k\text{-vertex-minor universal} \implies k \leq \delta_{\text{loc}}(G) + 1,$$

and  $k < \sqrt{2n \log_2 3} + 2$  for a  $k$ -vertex-minor universal graph of order  $n$ . The invariant  $\delta_{\text{loc}}$  is  $d - 1$ , where  $d$  is the minimum distance of the self-dual additive  $GF(4)$  code of the graph state (Section 2), so (2) makes the classification of such codes the natural source of candidates. Combining (2) with the classification of self-dual additive  $GF(4)$  codes of length at most 12 [14] — whose maximum distances are 1, 2, 2, 2, 3, 4, 3, 4, 4, 4, 5, 6 for  $n = 1, \dots, 12$  (also [20]) — and with the maximum-independent-set data that classification records for each local equivalence class, one gets  $\nu(5) \geq 13$ : at  $n \leq 10$  the distance is already too small, and each of the 65 classes of length 11 or 12 with  $d \geq 5$  has maximum independent set 4 over its orbit, whereas a 5-vertex-minor universal graph must realise the empty graph on some 5 vertices. This lower bound is not proved here; we use it only to say where the open interval lies.

**Results, over  $\mathbb{F}_2$ .** Our first result closes (1) by two.

**Theorem 1.2.** *There is a 5-vertex-minor universal graph of order 15; hence  $\nu(5) \leq 15$ .*

The witness is exhibited in Section 5 and certified by 8880 explicit local-complementation words, checked against all  $\binom{15}{5} \cdot 2^{10} = 3\,075\,072$  cells. Nothing about the search that produced the graph or the words enters the proof.

Our remaining results at  $p = 2$  concern the two orders left open, 13 and 14, and in particular the extremal codes at those lengths. Both rest on a blocking criterion which we prove from scratch in Section 6: local complementation acts on the graph-state code by a coordinatewise change of variables, restriction to  $S$  shortens that code along one  $\mathbb{F}_2$ -line per outside coordinate, and if no line assignment and no coordinatewise change of variables on  $S$  carries the shortened code into the code of a target  $F$ , then  $F$  is not a vertex-minor. The mathematics is classical — it is the binary form of Van den Nest, Dehaene and De Moor [19], and the elimination lemma of Bouchet [6] and Fon-Der-Flaass [16] is its graph-theoretic shadow — and none of it is claimed as new; what it buys here is that the negative statements below import nothing.

**Theorem 1.3.** *Let  $G_{14}$  be the graph of order 14 with graph6 string MAa\_OKrD]U1V|r}~?, one of the published extremal  $(14, 2^{14}, 6)$  Type II self-dual additive  $GF(4)$  codes. For every one of the  $\binom{14}{5} = 2002$  5-subsets  $S$  and every one of the  $2^{10}$  labelled graphs  $F$  on  $S$ :  $F$  is a vertex-minor of  $G_{14}$  if and only*

if  $(S, F)$  is not one of the twelve cells of Table 1. Hence  $\text{def}_5(G_{14}) = 12$ , where  $\text{def}_k$  counts unrealised cells, and  $G_{14}$  is not 5-vertex-minor universal. All twelve missing targets are labellings of  $2K_2 \cup K_1$ .

**Theorem 1.4.** *Neither the Paley graph of order 13 nor any of eight extremal order-13 graphs of code distance 5 — one drawn from each of eight slices of the order-13 candidate space, and chosen so that the cruder independence invariant of Section 7 does not decide them — is 5-vertex-minor universal.*

The Paley half of Theorem 1.4 is not a new value: it is asserted in [10] from numerical analysis and proved in [11] by a separability program; what is new is that it becomes a machine-checked certificate with no unformalised input. The eight order-13 statements are new.

**Results, over  $\mathbb{F}_p$ .** The second half of the paper replaces the field. A qudit graph state of prime dimension  $p$  is described by a symmetric zero-diagonal matrix  $M$  over  $\mathbb{F}_p$ , and Bahramgiri and Beigi [4, 5] give two operations on such matrices — a generalised local complementation  $*_a v$  and a local scaling  $\circ_b v$  — which generate exactly the local Clifford orbit. Transcribing Definition 1.1 with “graph” replaced by “ $\mathbb{F}_p$ -labelled graph” gives a quantity  $\nu_p(k)$  with  $\nu_2 = \nu$  (Section 9). Nothing about it appears to be in print: the framework exists, and the question is not asked.

Our first result on this axis is the one that needs no computation, and it holds at every prime at once.

**Theorem 1.5.** *Let  $p \geq 2$  be such that  $\mathbb{F}_p$  has no zero divisors. Then  $\nu_p(2) = 3$ : the triangle with all three labels equal to 1 is 2-vertex-minor universal over  $\mathbb{F}_p$ , and no  $\mathbb{F}_p$ -labelled graph on two vertices is.*

At  $p = 2$  this specialises to the published statement that  $K_3$  is the smallest 2-vertex-minor universal graph [11], so it is not a claim about the qubit value; what is new is every  $p > 2$  instance, and the uniformity. The remaining values were found by search and are certified cell by cell.

**Theorem 1.6.**  *$\nu_3(3) = 6$ , witnessed by the 6-cycle with every label 1;  $6 \leq \nu_3(4) \leq 10$ , the upper bound witnessed by the Petersen graph with every label 1; and  $5 \leq \nu_5(3) \leq 6$ , the upper bound witnessed by the same all-ones 6-cycle.*

The all-ones 6-cycle is a 3-vertex-minor universal  $\mathbb{F}_p$ -labelled graph for  $p = 2, 3, 5$  — literally the same matrix, verified three times — and the all-ones Petersen graph is 4-vertex-minor universal for  $p = 2$  and  $p = 3$ . Section 9.6 collects the values, adds what is computed outside the formal development, and asks whether  $\nu_p(k)$  depends on  $p$  at all.

**What is settled, and what is not.** The interval containing  $\nu(5)$  is not moved by this paper. Theorem 1.2 gives  $\nu(5) \leq 15$ ; the published lower bound is 13; a complete sweep of order 13, carried out outside the formal development and conditional on the length-12 classification, raises it to 14 (Remark 7.7). Theorem 1.3 is about one graph, and one graph failing says nothing about the rest of order 14. We record in Remark 8.5 what search was run there and what it cost. On the  $\mathbb{F}_p$  side, the two brackets of Theorem 1.6 are open at both ends of what is computable: the missing order-5 sweep at  $p = 5$  and the missing order-6 sweep at  $p = 3$  are each settled outside the formal development and are priced in Remark 9.9.

**Changes in version 2.** Two things are new since the first version of this paper. First, the negative statements at orders 13 and 14 no longer depend on an unformalised lemma. Version 1 proved twelve cells of  $G_{14}$  absent from a vertex-elimination recursion and concluded  $\text{def}_5(G_{14}) = 12$  only modulo the elimination lemma of Bouchet and Fon-Der-Flaass; and it stated the order-13 results as values of a line search, because the identity turning that value into a statement about vertex-minors was not formally proved. The criterion of Section 6 discharges both. Theorem 1.3 is now unconditional, Theorem 1.4 is now a statement about vertex-minors rather than about a search, and the earlier statements are kept, since they are proved by a genuinely different route and now serve as cross-checks (Theorem 8.4, Theorem 7.4). Second, Section 9 is entirely new: the  $\mathbb{F}_p$  layer, Theorems 1.5 and 1.6, and the question in Section 9.6. No theorem of version 1 is retracted or weakened, and two

things are narrowed. Version 1 sketched an elementary argument for both directions of (3) and (4); Section 2.3 now claims only the direction the paper uses — which Theorem 6.2 proves outright — and attributes the converses to Van den Nest. And the blanket “every statement is formally verified” is narrowed to the theorems and propositions, the computations reported in the remarks having always been outside the formal development.

**Related quantities.** Two recent papers [2, 9] study vertex-minor universality of random graphs; neither addresses small orders. A word of caution about a neighbouring invariant: the *vertex-minor Ramsey number*  $R_{\text{vm}}(k)$  of [2, 3] — the least  $n$  such that *every* graph of order  $n$  has the empty graph on  $k$  vertices as a vertex-minor — is a different quantity from  $\nu(k)$ . The two already differ at  $k = 4$ , where  $R_{\text{vm}}(4) = 11$  while  $\nu(4) = 10$ . In particular the open question whether  $R_{\text{vm}}(5) = 15$ , raised in [3], agrees numerically with Theorem 1.2 by coincidence, and nothing in this paper bears on  $R_{\text{vm}}$ .

## 2. PRELIMINARIES

**2.1. Local complementation, pivot, vertex-minor.** All graphs are finite, simple and labelled, with vertex set an initial segment  $\{0, 1, \dots, n-1\}$  unless stated otherwise. For a word  $w = u_1 u_2 \dots u_r$  over the vertex set we write  $G \star w = (\dots((G \star u_1) \star u_2) \dots) \star u_r$ . Local complementation is an involution,  $(G \star u) \star u = G$ , and  $G \star u = G$  whenever  $\deg_G(u) \leq 1$ , since there is then no pair inside  $N_G(u)$  to complement. The *pivot* along an edge  $uv$  is

$$G \wedge uv = G \star u \star v \star u,$$

and  $G - v$  denotes deletion of the vertex  $v$ . With this notation Definition 1.1 reads:  $G$  of order  $n$  is  $k$ -vertex-minor universal iff  $k \leq n$  and for every  $k$ -subset  $S$  and every labelled graph  $F$  on  $S$  there is a word  $w$  with  $(G \star w)[S] = F$ . Deleting the vertices outside  $S$  afterwards changes nothing, since the induced subgraph on  $S$  does not see adjacencies at deleted vertices; this is the equivalence of the two forms of the definition quoted in Section 1, and it is the reason the quantifier over deletions can be dropped.

**2.2. Codes of induced subgraphs.** It is convenient to identify a labelled graph on an ordered  $k$ -set  $S = (s_0, \dots, s_{k-1})$  with a single integer below  $2^{\binom{k}{2}}$ : the bit at position

$$\text{bp}(k, a, b) = \binom{k-1-a}{2} + (b-a-1) \quad (0 \leq a < b < k)$$

records whether  $s_a \sim s_b$ . We write  $\langle G \rangle_S$  for this integer, the *code* of  $G[S]$ , and  $\langle G \rangle = \langle G \rangle_{(0,1,\dots,n-1)}$  for the *graph code* of  $G$ . The map  $c \mapsto$  (the graph with code  $c$ ) is a bijection from  $\{0, 1, \dots, 2^{\binom{n}{2}} - 1\}$  onto the labelled graphs on  $n$  vertices; this is proved rather than assumed in our development (Proposition 3.2), so a statement quantified over codes really is a statement about all graphs. With this encoding, a cell is a pair  $(S, m)$  with  $m < 2^{\binom{k}{2}}$ , and universality is the assertion that the codes  $\langle G \star w \rangle_S$  exhaust  $\{0, \dots, 2^{\binom{k}{2}} - 1\}$  for each  $S$ .

**2.3. The graph-state code,  $\delta_{\text{loc}}$  and  $\alpha_{\text{loc}}$ .** Let  $\Gamma$  be the adjacency matrix of  $G$  over  $\mathbb{F}_2$ . The self-dual additive  $GF(4)$  code of the graph state of  $G$  is

$$C_G = \{ (x, \Gamma x) : x \in \mathbb{F}_2^n \},$$

coordinate  $i$  carrying the value  $x_i \omega + (\Gamma x)_i \in GF(4)$ . Its minimum distance is

$$d(G) = \min_{x \neq 0} |\text{supp}(x) \cup \text{supp}(\Gamma x)|,$$

and  $d(G) = \delta_{\text{loc}}(G) + 1$ , an identity we verified exhaustively against the definition of  $\delta_{\text{loc}}$  as a minimum over the local equivalence class, at every labelled graph of order at most 7; local complementation acts on  $C_G$  by a coordinatewise change of variables (Section 6), so  $d$  is a local-equivalence invariant, and (2) becomes the requirement  $d(G) \geq k$ . We write  $\alpha_{\text{loc}}(G)$  for the largest independent set over the whole local equivalence class of  $G$ ; since the empty graph on  $k$  vertices must be a vertex-minor of a  $k$ -vertex-minor universal graph,  $\alpha_{\text{loc}}(G) \geq k$  is a second necessary condition.

At each coordinate  $i$  there are three  $\mathbb{F}_2$ -lines in the fibre, and choosing one at every coordinate cuts  $C_G$  down to a subspace  $D_L = \{x : r_i \cdot x = 0 \text{ for all } i\}$ , where  $r_i$  runs over  $\{e_i, \Gamma_i, e_i + \Gamma_i\}$  ( $\Gamma_i$  being row  $i$  of  $\Gamma$ ). Two invariants are read off these subspaces; both are used below and both are computable in  $3^n$  steps rather than by walking an orbit:

$$(3) \quad \alpha_{\text{loc}}(G) = n - \min\{\text{rank}_{\mathbb{F}_2}(r_0, \dots, r_{n-1}) : r_i \in \{e_i, \Gamma_i, e_i + \Gamma_i\}\},$$

(4)

$S$  can be made independent by local complementations  $\iff S$  is an information set of some  $D_L$ .

Here “ $S$  is an information set of  $D_L$ ” means that  $x \mapsto (f_i \cdot x)_{i \in S}$  is onto  $\mathbb{F}_2^S$ , where  $f_i$  is the functional detecting that coordinate  $i$  of the codeword is nonzero:  $f_i = \Gamma_i$  for the line  $x_i = 0$  and  $f_i = e_i$  for the other two. Equivalently, no nonempty subset sum of  $\{f_i : i \in S\}$  lies in  $\text{span}\{r_0, \dots, r_{n-1}\}$ . Neither (3) nor (4) is formally proved here as an equivalence for general  $n$ ; the direction this paper actually uses — the “only if” of (4), which is what turns a failed search into a negative statement — is a special case of the criterion of Section 6 and is proved there at every  $n$ , with no target restriction. The converses are Van den Nest’s theorem and remain outside our development.

### 3. TWO SHAPES OF CERTIFICATE

Every statement in this paper is reduced to a finite check, and no check trusts the search that produced its data.

**3.1. Covering families (positive).** A *covering family* for  $(n, k, G)$  is a list  $w_1, \dots, w_N$  of words over  $V(G)$  such that for every  $k$ -subset  $S$  the codes  $\langle G \star w_1 \rangle_S, \dots, \langle G \star w_N \rangle_S$  run over all of  $\{0, \dots, 2^{\binom{k}{2}} - 1\}$ . Checking one is a fixed computation: apply each word, take the induced code on each subset, and accumulate one bitmask per subset. Since each word supplies at most one target per subset,  $N \geq 2^{\binom{k}{2}}$  always.

**3.2. Blocking certificates (negative).** A *blocking certificate* at order  $n$  for degree  $k$  assigns to every one of the  $2^{\binom{n}{2}}$  labelled graphs on  $n$  vertices a cell, in such a way that (i) the assignment is unchanged by a single local complementation and (ii) no graph realises its own assigned cell. Invariance plus induction along a word then gives  $\neg(k\text{-vertex-minor universal})$  for *every* graph of order  $n$  at once, from the  $n \cdot 2^{\binom{n}{2}}$  local complementations that the invariance check performs.

**Proposition 3.1** (the two bridges). *A verified covering family for  $(n, k, G)$  implies that  $G$  is  $k$ -vertex-minor universal. A verified blocking certificate at order  $n$  for degree  $k$  implies that no graph of order  $n$  is  $k$ -vertex-minor universal, and in its sharp form names, for each graph, a cell that no graph in its local equivalence class realises. Moreover, deleting vertices outside  $S$  leaves the induced code on  $S$  unchanged, so the two forms of the definition of vertex-minor agree.*

*Proof sketch.* The positive direction is one lemma: a set bit of the accumulated mask exhibits an index, hence a word. The negative direction is an induction on the length of the word, using invariance of the assignment under a single local complementation, together with the observation that the graphs reachable from a code are again codes. The last statement is a congruence: the code  $\langle \cdot \rangle_S$  reads only adjacencies inside  $S$ .  $\square$

**Proposition 3.2.** *For every  $n$ , the decoding map  $c \mapsto (\text{the graph with code } c)$  is a bijection from  $\{0, \dots, 2^{\binom{n}{2}} - 1\}$  onto the labelled graphs on  $n$  vertices; in particular a statement proved for all  $c$  below  $2^{\binom{n}{2}}$  holds for every graph of order  $n$ .*

*Proof sketch.* Bit  $\text{bp}(n, i, j)$  of  $\langle G \rangle$  is the adjacency of  $i$  and  $j$ , which gives the left inverse; the decoded array is symmetric, loop-free and has rows below  $2^n$ , which gives the right inverse. Both are elementary bit manipulations, proved for general  $n$ .  $\square$

4. EXACT VALUES AT  $k \leq 3$ , AND THE ANCHORS AT  $k = 4$ 

**Theorem 4.1.**  $\nu(2) = 3$  and  $\nu(3) = 6$ . *Precisely: no graph on 2 vertices is 2-vertex-minor universal and  $K_3$  is; no graph on 3, 4 or 5 vertices is 3-vertex-minor universal and  $C_6$  is.*

*Proof sketch.* The positive halves are covering families of 3 and 23 words respectively. The negative halves are blocking certificates over all 2, 8, 64 and 1024 labelled graphs of orders 2, 3, 4, 5; by Proposition 3.2 these are statements about every graph of those orders. The source argues the  $k = 3$  lower half instead through the orbit database of [1], the filter  $\delta_{\text{loc}} \geq 2$  and one orbit computation on  $C_5$ ; the present argument uses none of those.  $\square$

**Proposition 4.2.** *The Möbius ladder  $C_{10}(1, 5)$ , the Petersen graph, and the Paley graph of order 13 are all 4-vertex-minor universal, and no graph of order at most 6 is.*

The three positive claims are the source’s, asserted there from numerical observation; here they are covering families of 260, 282 and 382 words against a floor of 64. The lower half is certified here only up to order 6: the published statement that no graph of order 9 or less is 4-vertex-minor universal is an inference from the 2-pairability result of [7] and is not reproduced. We note that the source’s “wheel” is the Möbius ladder  $C_{10}(1, 5)$ , i.e.  $N(j) = \{j - 1, j + 1, j + 5\}$  for  $j \in \mathbb{Z}_{10}$ ; this reading is forced both by the figure in [10] and by the stabilizer generators  $S_j = X_j Z_{j-1} Z_{j+1} Z_{j+5}$  printed in [7].

**Proposition 4.3** (controls).  *$C_5$  is not 3-vertex-minor universal, and no sequence of local complementations makes  $\{0, 1, 2\}$  independent in it.  $C_6$  is not 4-vertex-minor universal, and no sequence makes  $\{0, 1, 2, 3\}$  independent in it.  $K_3$  is not 4-vertex-minor universal. Furthermore the certificate check rejects the empty family, a family with one word removed, a  $k = 3$  family presented at  $k = 4$ , and a named wrong witness; and the graph codes of the Petersen graph and of  $C_{10}(1, 5)$  agree with the values printed by the independent search program used to find the certificates.*

The first of these recovers, as a statement about every word rather than as an orbit computation, the source’s own justification that  $C_5$  is not 3-vertex-minor universal (“checking that none of them contains an independent set of size 3”). The second refutes a too-large claim ( $C_6$  is 3- but not 4-vertex-minor universal), the third shows that the condition  $k \leq n$  in Definition 1.1 is not vacuous, and the remaining items are falsification tests for the checker itself.

5. AN ORDER-15 WITNESS AT  $k = 5$ 

**Theorem 5.1.** *Let  $G_{15}$  be the graph on  $\{0, 1, \dots, 14\}$  with the following 59 edges, listed as the neighbours of each vertex among the later vertices:*

0: 1, 2, 10, 11, 12, 13, 14; 1: 2, 5, 7, 8, 9, 10, 11, 12; 2: 3, 4, 5, 7, 10, 11, 12, 13; 3: 4, 6, 8, 13, 14;  
4: 5, 6, 7, 9, 11, 13; 5: 6, 8, 9, 11, 14; 6: 10, 11, 13; 7: 8, 9, 11, 12, 13, 14; 8: 9, 10, 13; 9:  
10, 12, 13, 14; 10: 14; 11: 12, 14; 13: 14.

*Then  $G_{15}$  is 5-vertex-minor universal: for every 5-subset  $S \subseteq \{0, \dots, 14\}$  and every labelled graph  $F$  on  $S$  there is a word  $w$  with  $(G_{15} \star w)[S] = F$ . Consequently  $\nu(5) \leq 15$ .*

*Proof sketch.* A covering family of 8880 words, each of length 24, is exhibited and verified. The verification is a single finite computation: apply each of the 8880 words to  $G_{15}$ , and for each of the  $\binom{15}{5} = 3003$  subsets accumulate the induced codes into a 1024-bit mask; the claim is that all 3003 masks are full, i.e. that all  $3003 \cdot 2^{10} = 3\,075\,072$  cells are covered. The passage from the Boolean to the existential statement is Proposition 3.1, whose only content is that a set bit exhibits an index.

How the data was found is irrelevant to the proof, and we record it only for reproducibility. Candidate graphs of order 15 were drawn at random and hill-climbed on  $\delta_{\text{loc}}$  until they met the necessary condition (2), i.e.  $\delta_{\text{loc}} \geq 4$ ; of the 238 candidates that passed that filter, 4 covered all 3003 subsets under a random-walk coverage test. The graph above was re-tested from an independent seed (coverage complete after 439 012 steps) before any certificate was built. The covering family itself was assembled from words of *fixed* length 24 drawn at random, rather than from the prefixes of one long random

walk, so that each witness costs 24 local complementations to replay; a breadth-first ball of radius 6 around  $G_{15}$  (193 304 graphs) is not diverse enough, reaching only 2170 of the 3003 subsets.  $\square$

**Proposition 5.2.** *The Paley graph of order 17 is 5-vertex-minor universal.*

*Proof sketch.* A covering family of 9124 words against all  $\binom{17}{5} \cdot 2^{10} = 6\,336\,512$  cells. This is the claim behind (1); the source asserts it from “numerical analysis”, and an earlier attempt to settle it by orbit search here stopped undecided at 99.16% coverage of an orbit capped at  $8 \cdot 10^6$  elements. A covering family needs no orbit at all, which is the practical point of the positive certificate shape. As a consistency check on the source’s own numbers,  $\delta_{\text{loc}}$  of the Paley graph of order 17 is 4, so (2) gives  $k \leq 5$ , matching the source’s “5-vertex-minor universal but not 6-”.  $\square$

## 6. A BLOCKING CRITERION FROM THE GRAPH-STATE CODE

Sections 7 and 8 need to say, of a specific graph and a specific target, that *no* word of local complementations realises it. A blocking certificate in the sense of Section 3 cannot do this above order 6, since it enumerates all  $2^{\binom{n}{2}}$  graphs. The following criterion does, one cell at a time, and it is the technical heart of the negative half of this paper.

Write  $\Gamma$  for the adjacency matrix of  $G$  over  $\mathbb{F}_2$  and  $C_G = \{(x, \Gamma x)\}$  for the graph-state code of Section 2.3, coordinate  $i$  carrying the pair  $(x_i, (\Gamma x)_i)$  of  $X$ - and  $Z$ -exponents.

**Proposition 6.1.** *Let  $u \in V(G)$  and let  $\sigma_u$  be the coordinatewise  $\mathbb{F}_2$ -linear map that is  $(a, b) \mapsto (a+b, b)$  at  $u$ ,  $(a, b) \mapsto (a, a+b)$  at every  $w \in N_G(u)$ , and the identity elsewhere. Then  $\sigma_u(C_G) = C_{G \star u}$ ; explicitly, with  $\varphi(x) = x + (\Gamma x)_u e_u$  and  $\Gamma'$  the adjacency of  $G \star u$ ,*

$$\Gamma'(\varphi x) = \Gamma x + (\Gamma_u \wedge x) \quad (x \in \mathbb{F}_2^n),$$

*and  $\varphi$  is an involution of  $\mathbb{F}_2^n$ . Consequently, for every word  $w$  there are bitmasks  $A, B, C, D$  with  $A_i D_i + B_i C_i = 1$  at every coordinate  $i < n$  such that  $(C \wedge x) + (D \wedge \Gamma x) = \Gamma_{G \star w}((A \wedge x) + (B \wedge \Gamma x))$  for all  $x$ , the map  $x \mapsto (A \wedge x) + (B \wedge \Gamma x)$  being onto  $\mathbb{F}_2^n$ .*

**Theorem 6.2.** *Let  $S \subseteq V(G)$  with  $|S| = k$  and let  $F$  be a labelled graph on  $S$ . Suppose that for every one of the  $3^{n-k}$  assignments of one  $\mathbb{F}_2$ -line*

$$x_v = 0, \quad (\Gamma x)_v = 0, \quad x_v + (\Gamma x)_v = 0$$

*to each  $v \notin S$ , and for every coordinatewise  $\tau \in GL_2(\mathbb{F}_2)^S$ , the code shortened by that assignment is not carried into  $C_F$  by  $\tau$ . Then  $(G \star w)[S] \neq F$  for every word  $w$ ; that is,  $F$  is not a vertex-minor of  $G$ .*

*Proof sketch.* Proposition 6.1 is one bitwise case split, proved for general  $n$ : for  $i \notin N(u)$  row  $i$  is unchanged and the extra term  $(\Gamma x)_u \Gamma_{iu}$  vanishes; for  $i \in N(u)$  row  $i$  becomes  $\Gamma_i + \Gamma_u + e_i$ , which pairs against  $\varphi x$  to  $(\Gamma x)_i + x_i$ , and  $i \neq u$  because  $\Gamma_{uu} = 0$ . The composed form follows by induction on  $w$  from the composition law for coordinatewise maps and multiplicativity of the  $2 \times 2$  determinant over  $\mathbb{F}_2$ , a finite case check. For the criterion, restricting a graph  $H$  to  $S$  keeps exactly the codewords of  $C_H$  whose  $X$ -part vanishes outside  $S$ ; pulled back along the composed map, the condition at  $v \notin S$  reads  $A_v x_v + B_v (\Gamma x)_v = 0$  with  $(A_v, B_v) \neq (0, 0)$  (the determinant is 1), hence is one of the three lines — these are the three Pauli measurement bases at  $v$ , which is why the elimination lemma of Bouchet [6] and Fon-Der-Flaass [16] has three children. What survives, read on  $S$ , is the image of the shortened code under the restriction of the composed map to  $S$ , a coordinatewise element of  $GL_2(\mathbb{F}_2)^S$ .

Two points make the check a certificate rather than a search. The Gaussian elimination that produces a basis of the shortened code is *untrusted*: every vector it returns is re-verified against every line functional before use, and a vector it fails to return only weakens the check. And the enumeration of the  $6^k$  coordinatewise maps is proved complete — every quadruple of  $k$ -bit masks with determinant one at each coordinate occurs — from the finite fact that  $GL_2(\mathbb{F}_2)$  is exactly the six  $2 \times 2$  binary matrices of determinant one.  $\square$

The mathematics of Proposition 6.1 is the binary form of the description of local Clifford action on graph states of Van den Nest, Dehaene and De Moor [19], and Theorem 6.2 is a certificate form of the elimination lemma. *Nothing in this section is claimed as new mathematics*; what is new is that it is proved rather than cited, so that Theorems 7.5, 7.6 and 8.2 import nothing. The criterion is proved *sound*. It is not proved exact, and no statement below needs it to be; exactness is instead measured.

**Proposition 6.3** (exactness, measured). *Over all 1024 labelled graphs of order 5 and all 8 labelled graphs on  $\{0, 1, 2\}$ , the criterion of Theorem 6.2 returns “blocked” exactly at the cells that the local-complementation orbit does not reach.*

*Proof sketch.* The orbit side is computed from the definition, by propagating the induced code along single local complementations until the propagation stops changing; a companion check certifies that the fixed point was reached, so no truncated orbit is trusted. Outside the formal development the same comparison was run over *every* labelled graph of orders 5, 6 and 7 at  $k = 3$ , and of orders 6 and 7 at  $k = 4$  — 153 362 432 cells over those five pairs  $(n, k)$  — with zero mismatches.  $\square$

**Proposition 6.4** (controls). *The criterion does not block the empty triple in  $C_6$ , nor the empty quadruple in the Petersen graph, both of which are vertex-minors because those graphs are 3- and 4-vertex-minor universal (Theorem 4.1, Proposition 4.2); nor does it block the empty graph on  $\{1, 2, 5, 6, 11\}$  in the order-14 graph of Section 8, for which Theorem 8.1 exhibits a word. It is also not vacuously negative: on the subset  $\{0, 1, 2, 3, 4\}$  of that graph it does not block the target it blocks on  $\{1, 2, 5, 6, 11\}$ . Finally the check is never empty: over the 19 683 line assignments for  $\{1, 2, 5, 6, 11\}$  the untrusted elimination step returns five verified vectors at 19 494 of them and six at the 189 where the nine line functionals are dependent, and never zero.*

These refute the two failure modes a sound-but-useless criterion has — blocking everything, and blocking nothing — and, with Proposition 6.3, are why a verdict of “blocked” is worth reporting.

## 7. THE LINE INVARIANT, AND ORDER 13

Order 13 is the first order at which  $\alpha_{\text{loc}}$  alone stops deciding the question. At length 12 every class with  $d \geq 5$  has  $\alpha_{\text{loc}} = 4$ , which is what gives the published bound  $\nu(5) \geq 13$ ; at order 13, all but 0.57% of the 3 450 170 candidates with  $d \geq 5$  described in Remark 7.7 have  $\alpha_{\text{loc}} = 5$ , so some 5-subset can be emptied in almost all of them and the question becomes which subsets. The refinement (4) answers that one subset at a time.

**Proposition 7.1.** *The identity (3) holds at every labelled graph of order  $n \leq 6$ .*

*Proof sketch.* Both sides are computed at all  $2^{\binom{n}{2}}$  labelled graphs for  $n = 2, \dots, 6$  and compared. The orbit side is obtained by propagating the ordinary independence number along single local complementations until the propagation stops changing, and a companion check certifies that the fixed point was reached, so no orbit enumeration is trusted. Outside the formal development the same identity was checked against the published maximum-independent-set column for all 1 373 462 self-dual additive  $GF(4)$  codes of length at most 12, with zero mismatches. The identity itself is *not* proved here for general  $n$ ; the direction the paper uses is Theorem 6.2 at the empty target.  $\square$

**Proposition 7.2.** *For the Paley graph  $P_{13}$  of order 13, the minimum in (3) equals 9, so the right-hand side of (3) is  $13 - 9 = 4$ . For the Petersen graph the value is 5, for  $C_5$  it is 2, and for  $K_3$  it is 2.*

Read through (3), the first of these says  $\alpha_{\text{loc}}(P_{13}) = 4$ , i.e. that the empty graph on 5 vertices is not a vertex-minor of  $P_{13}$ ; this is the invariant behind the claim, asserted in [10] and proved in [11] by a separability argument, that  $P_{13}$  is not 5-vertex-minor universal. Theorem 7.5 below proves that claim outright. The remaining three values agree with the published maximum-independent-set column, the  $C_5$  value being the source’s own sentence about  $C_5$ .

**Proposition 7.3** (controls). *The invariant is not the ordinary independence number: the two differ at 266 of the 1024 labelled graphs on 5 vertices, and at  $K_3$  itself (1 against 2). The right-hand side of (3) at the Paley graph of order 13 is not 5. And the construction is not over-general: dropping the third line  $\{0, \omega^2\}$  from the choice at each coordinate already gives the wrong answer at  $K_3$ , where the winning choice is  $e_i + \Gamma_i$  at every vertex.*

**Theorem 7.4.** *Let  $H_1, \dots, H_8$  be the graphs of order 13 with graph6 strings*

LKGOt?\OqW{p}I LA\_oAQaNrtz{j? LKx@?KXaPlyvsg LDGBCOMSYw{1`}  
LlCg@ORQ\_Nrq~h LBw@YGgc]`uzvc L@drQ\_`oHrtevh LqC?@CMAziv}r^

*Each has code distance  $d(H_i) = 5$ , and the right-hand side of (3) equals 5 at each of them, so the invariant of Proposition 7.2 does not decide them. For each  $i$ , no choice of one  $\mathbb{F}_2$ -line per coordinate makes  $\{0, 1, 2, 3, 4\}$  an information set of the resulting subspace of  $C_{H_i}$ . The same holds for  $P_{13}$  at  $k = 5$ , for  $C_5$  at  $k = 3$  and for  $C_6$  at  $k = 4$ ; and, as it must, the search does find a line assignment for  $C_6$  at  $k = 3$ , for the Petersen graph at  $k = 4$  and for  $P_{13}$  at  $k = 4$ .*

*Proof sketch.* The search is a depth-first assignment of one line per coordinate, carrying the partial row space  $R = \text{span}\{r_i\}$  and the partial subset sums of the functionals  $\{f_i : i \in S\}$ . Since  $R$  only grows as the search descends, a subset sum already inside the partial  $R$  can never leave it, which prunes the  $3^{13}$  tree to 10 452 nodes at  $P_{13}$  and to 247–271 nodes at the  $H_i$ . The prune is sound but not complete, so the verdict at a leaf is re-taken against the final  $R$ ; a control in the development exhibits a graph on which trusting the prune unretested gives the wrong answer. The values  $d(H_i) = 5$  and the value 5 of the right-hand side of (3) are separate finite computations, and they are what make the statement non-vacuous: each  $H_i$  satisfies the necessary condition (2), and the invariant of Proposition 7.2 does not decide it.  $\square$

Theorem 7.4 is a statement about a line search. The criterion of Section 6 turns the same computation, run over the full  $3^{n-k} \times 6^k$  table rather than with the pruning above, into a statement about vertex-minors.

**Theorem 7.5.** *The empty graph on  $\{0, 1, 2, 3, 4\}$  is not a vertex-minor of the Paley graph of order 13. Hence  $P_{13}$  is not 5-vertex-minor universal.*

**Theorem 7.6.** *For each of the eight graphs  $H_1, \dots, H_8$  of Theorem 7.4, the empty graph on the subset  $\{0, 1, 2, 3, 4\}$  is not a vertex-minor of  $H_i$ . Hence none of the eight graphs is 5-vertex-minor universal.*

*Proof sketch.* Nine applications of Theorem 6.2 with  $F$  the empty graph: at  $P_{13}$  over all  $3^8 = 6561$  line assignments, at each  $H_i$  over the same  $3^8$ , and in each case over all  $6^5 = 7776$  coordinatewise maps. Each is one finite evaluation. The verdicts are cross-checked in the formal development against the line search of Theorem 7.4 — an unrelated algorithm, with no line-assignment sweep and no coordinatewise closure in it — on all sixteen graphs where that search has a verdict, with both verdicts occurring; together with Proposition 6.3 this is the evidence that the criterion is neither reporting spurious blocks nor agreeing with itself by convention. The value of  $P_{13}$  here is the source’s own claim, and [11] proves it by a separability program after recording that the local-complementation orbit of  $P_{13}$  is too large to compute; what is new is the route.  $\square$

*Remark 7.7.* The eight graphs above are not arbitrary. Outside the formal development, the whole order-13 candidate space was regenerated by Varbanov’s own lengthening construction [22] from the published length-12 classification [14] — all 195 520 length-12 parents with  $d \geq 4$ , yielding 3 450 170 order-13 candidates with  $d \geq 5$  — and swept. Not one is 5-vertex-minor universal; the maximum number of 5-subsets that the emptiability filter passes is 1277 of 1287, attained by exactly 41 candidates, with nothing anywhere at 1278. The  $H_i$  are eight of those, one from each of eight different slices of the parent set, relabelled so that a blocked subset is  $\{0, 1, 2, 3, 4\}$ . The conclusion *no graph of order 13 is 5-vertex-minor universal*, and hence  $\nu(5) \geq 14$ , is therefore conditional on the completeness of the length-12 classification, and it is a computation, not a theorem of this paper. Certifying it cell by cell with Theorem 6.2 is not out of the question but is out of budget: the sweep alone is 57 CPU-hours in C.

## 8. ORDER 14: THE DEFICIT OF AN EXTREMAL GRAPH

**8.1. The graph.** Let  $G_{14}$  be the graph of order 14 with graph6 string `MAa_0KrD]U1V|r}~?`, one of the 1020 inequivalent extremal  $(14, 2^{14}, 6)$  Type II self-dual additive  $GF(4)$  codes classified by Danielsen and Parker [14] — the same count was obtained independently by Varbanov [22] — and published as graph representatives in [15]. Its 48 edges, in the same notation, are

0: 4, 5, 10, 12, 13; 1: 3, 10, 11, 12, 13; 2: 5, 8, 11, 12, 13; 3: 8, 9, 12, 13; 4: 6, 10, 11, 13; 5: 7, 9, 12;  
6: 7, 8, 10, 11, 12, 13; 7: 8, 9, 10, 12, 13; 8: 9, 11, 13; 9: 10, 11, 13; 10: 11, 12, 13; 11: 12, 13.

Its degree sequence is  $(5, 5, 5, 5, 5, 5, 7, 7, 7, 7, 9, 9, 9, 11)$ , and its code distance is  $d(G_{14}) = 6$ , so  $\delta_{\text{loc}}(G_{14}) = 5$  and (2) permits  $k = 5$ . Both the decoding of the graph6 string into the adjacency rows and the value  $d(G_{14}) = 6$  are part of the formal development, so the object studied here is pinned to the published one and not to a transcription of it. For a graph  $G$  of order  $n$  write  $\mathcal{M}_S(G)$  for the set of labelled graphs on  $S$  that are vertex-minors of  $G$ , and put

$$(5) \quad \text{def}_k(G) = \sum_{|S|=k} \left( 2^{\binom{k}{2}} - |\mathcal{M}_S(G)| \right),$$

so that  $\text{def}_k(G) = 0$  if and only if  $G$  is  $k$ -vertex-minor universal.

**8.2. The positive half.**

**Theorem 8.1.** *For every one of the  $\binom{14}{5} = 2002$  5-subsets  $S$  of  $V(G_{14})$  and every labelled graph  $F$  on  $S$  outside the twelve cells listed in Table 1, there is a word  $w$  with  $(G_{14} \star w)[S] = F$ . This covers 2 050 036 of the 2 050 048 cells and uses 7233 words. In particular*

$$\text{def}_5(G_{14}) \leq 12.$$

*Moreover, at the single subset  $S = \{1, 2, 5, 6, 11\}$ , all 1023 labelled graphs on  $S$  other than the one with edges  $\{1, 5\}$ ,  $\{2, 6\}$  and 11 isolated are vertex-minors of  $G_{14}$ , one word each.*

*Proof sketch.* The check is the one of Section 3: each of the 7233 words is applied to  $G_{14}$ , its induced code on each subset is read off, and the accumulated masks are compared against “full, except the twelve named cells”. There is no auxiliary lemma: the only step from the Boolean value to the existential statement is that a set bit exhibits an index. Each realised code is a genuine vertex-minor because the deletions outside  $S$  may be postponed (Proposition 3.1), so the bound on  $\text{def}_5$  is unconditional.

The words were extracted from the leaves of the elimination recursion of Section 8.3 — the operations along a root-to-leaf path concatenate into a single word — and then reduced by a batch-greedy set cover; none of that search enters the proof. Three checks control slackness and correctness of the data. The same 7233 words realise *none* of the twelve cells, so the complement of the certificate is exactly Table 1 and not a superset; the first 6000 words leave 62 cells of those twelve subsets unrealised, against 12 for all 7233, so the tail of the cover is load-bearing; and replaying the same words on the graph obtained from  $G_{14}$  by toggling the single pair  $\{0, 1\}$  leaves 78 cells unrealised, so the words are checked against  $G_{14}$  and not against an arbitrary graph. At  $S = \{1, 2, 5, 6, 11\}$  a separate 1023-word family is verified, and removing one of its words leaves exactly two cells unrealised, so it too is tight.  $\square$

**8.3. The negative half.**

**Theorem 8.2.** *For each of the twelve pairs  $(S, F)$  of Table 1 and every word  $w$ ,  $(G_{14} \star w)[S] \neq F$ ; that is, none of the twelve targets is a vertex-minor of  $G_{14}$ . Consequently, for every 5-subset  $S$  and every labelled graph  $F$  on  $S$ ,*

$$F \in \mathcal{M}_S(G_{14}) \iff (S, F) \notin \text{Table 1},$$

*so  $\text{def}_5(G_{14}) = 12$  and  $G_{14}$  is not 5-vertex-minor universal. (The displayed equivalence and the non-universality are the machine-checked statements; reading the value 12 off the equivalence is a count of the rows of Table 1.)*

TABLE 1. The twelve cells of  $G_{14}$ . Every missing target is  $2K_2 \cup K_1$ ; only seven distinct pairs of disjoint edges occur.

| $S$                    | edges of $F$           | isolated | $S$                    | edges of $F$           | isolated |
|------------------------|------------------------|----------|------------------------|------------------------|----------|
| $\{0, 3, 5, 12, 13\}$  | $\{3, 5\}, \{12, 13\}$ | 0        | $\{3, 5, 6, 8, 10\}$   | $\{3, 8\}, \{6, 10\}$  | 5        |
| $\{1, 2, 5, 6, 11\}$   | $\{1, 5\}, \{2, 6\}$   | 11       | $\{3, 5, 7, 12, 13\}$  | $\{3, 5\}, \{12, 13\}$ | 7        |
| $\{1, 8, 9, 10, 12\}$  | $\{1, 12\}, \{8, 10\}$ | 9        | $\{3, 5, 9, 12, 13\}$  | $\{3, 5\}, \{12, 13\}$ | 9        |
| $\{2, 3, 9, 10, 11\}$  | $\{2, 11\}, \{3, 10\}$ | 9        | $\{3, 5, 11, 12, 13\}$ | $\{3, 5\}, \{12, 13\}$ | 11       |
| $\{2, 6, 9, 10, 13\}$  | $\{2, 13\}, \{6, 10\}$ | 9        | $\{3, 6, 8, 10, 11\}$  | $\{3, 8\}, \{6, 10\}$  | 11       |
| $\{2, 6, 10, 12, 13\}$ | $\{2, 13\}, \{6, 10\}$ | 12       | $\{6, 8, 9, 11, 13\}$  | $\{6, 13\}, \{8, 9\}$  | 11       |

*Proof sketch.* Twelve applications of Theorem 6.2, each a single finite evaluation over all  $3^9 = 19683$  line assignments and all  $6^5 = 7776$  coordinatewise maps. The stated equivalence combines these with Theorem 8.1, whose 7233 words supply the converse direction at every other cell; both halves are unconditional, which is what makes the value of  $\text{def}_5$  exact rather than an upper bound. Proposition 6.4 is what rules out the failure mode a negative computation has here, namely a criterion that blocks indiscriminately: its three items are stated at exactly this graph and these subsets. The twelve cells were independently recomputed, cell for cell, by a C program working from the code side and sharing no algorithm with the formal development.  $\square$

**8.4. The same twelve cells, by vertex elimination.** The three-way vertex elimination is the graph form of the three Pauli measurement bases at a removed qubit, and it was the route by which the twelve cells were first found. We keep it because it is an independent computation of the same fact.

**Lemma 8.3** (elimination lemma; Bouchet [6], Fon-Der-Flaass [16]). *Let  $S \subseteq V(G)$  and  $v \in V(G) \setminus S$ . If  $v$  is isolated then  $\mathcal{M}_S(G) = \mathcal{M}_S(G - v)$ ; otherwise, for any neighbour  $u$  of  $v$ ,*

$$\mathcal{M}_S(G) = \mathcal{M}_S(G - v) \cup \mathcal{M}_S((G \star v) - v) \cup \mathcal{M}_S((G \wedge uv) - v).$$

*When  $V(G) = S$ ,  $\mathcal{M}_S(G)$  is the local equivalence class of  $G$  inside  $S$ .*

The inclusion  $\supseteq$  is immediate in our setting: each of the three children is reached from  $G$  by an explicit word  $(\varepsilon, v, uvu)$  followed by a deletion outside  $S$ , and deletions outside  $S$  may be postponed. The inclusion  $\subseteq$  is the substantive half; it was proved independently by Bouchet [6], by way of isotropic systems, and by Fon-Der-Flaass [16], in graph-theoretic terms. The form we use it in — if  $H$  is a vertex-minor of  $G$  and  $v \in V(G) \setminus V(H)$ , then  $H$  is a vertex-minor of one of  $G - v$ ,  $(G \star v) - v$  and  $(G \wedge vw) - v$  — is the one stated, with both attributions, in the survey of Kim and Oum [17], which also records that the pivot neighbour  $w$  may be chosen freely, since  $(G \wedge vw) - v$  and  $(G \wedge vw') - v$  are pivot-equivalent for distinct neighbours  $w, w'$  of  $v$ . *It is not part of our formal development.* It was the only external ingredient of this section in the first version of this paper; Theorem 8.2 has since replaced it, and Theorem 8.4 below is stated so that it needs no lemma at all.

Fix an elimination order on  $V(G_{14}) \setminus S$  (we take increasing vertex index) and a pivot rule (the lowest-index neighbour). Let  $\mathcal{R}_S(G)$  denote the set of labelled graphs on  $S$  produced by unfolding the right-hand side of Lemma 8.3 along that order and closing the resulting leaves under local complementation inside  $S$ . Then  $\mathcal{R}_S(G) \subseteq \mathcal{M}_S(G)$  unconditionally, and  $\mathcal{M}_S(G) = \mathcal{R}_S(G)$  given Lemma 8.3. Since  $|S| = 5$  and  $|V(G_{14})| = 14$ , the tree has at most  $3^9 = 19683$  leaves.

**Theorem 8.4.** *For each of the twelve pairs  $(S, F)$  of Table 1,*

$$\mathcal{R}_S(G_{14}) = \{\text{all labelled graphs on } S\} \setminus \{F\},$$

*and  $F$  occurs at none of the leaves of the elimination tree. Each of the twelve  $F$  is a labelling of  $2K_2 \cup K_1$ . In particular, for  $S = \{1, 2, 5, 6, 11\}$  the missing graph is the one with edges  $\{1, 5\}$  and  $\{2, 6\}$  and vertex 11 isolated, absent from all 19305 leaves of that tree.*

*Proof sketch.* Each of the twelve statements is a single finite computation: unfold the elimination tree at  $S$ , collect the codes of the leaves, close the resulting mask under the five local complementations inside  $S$ , and report which codes are absent. At  $S = \{1, 2, 5, 6, 11\}$  the tree has 19 305 leaves rather than 19 683, because an isolated vertex branches once instead of three ways; its 981 distinct leaf codes close to 1023 of the 1024 targets. A control verifies that the closure has actually reached a fixed point, which matters because a truncated closure would under-approximate  $\mathcal{R}_S$  and so would be unsound for a negative statement. Read through Lemma 8.3, this recovers Theorem 8.2; the two computations share no code, and they agree cell for cell.  $\square$

**8.5. Why the obstruction sits on  $2K_2 \cup K_1$ .** Local complementation at a vertex of degree at most 1 is the identity, so every matching is a fixed point of every local complementation, and in particular each of the 26 matchings on 5 labelled vertices (1 empty, 10 single-edge, 15 two-edge) is a singleton local equivalence class. There are 93 classes in all at  $k = 5$ , and a finite check of them confirms that these 26 are the only singletons. Two consequences shape the computation above. First, a cell whose target is a matching must be missed by *every* leaf individually — the closure step cannot supply it — which is what makes Theorem 8.4 sharp; the development checks the relevant instance, that all five local complementations inside  $S$  fix the code of  $2K_2 \cup K_1$  on  $\{1, 2, 5, 6, 11\}$ . Second, the linear-algebraic filter of Section 7 tests one target, the empty graph, which is one singleton class out of 26 and the easiest; it is structurally blind to the two-edge matchings, and that is why the order-14 obstruction was not visible to it. Table 1 bears this out from the other side: the twelve missing targets use only seven distinct pairs of disjoint edges, and the pair  $\{3, 5\}, \{12, 13\}$  alone accounts for four of the twelve. The same signature appears at order 13: run over the whole grid rather than at one target, the criterion of Section 6 reports that  $P_{13}$  reaches 1017 of the 1024 labelled graphs on  $\{0, 1, 2, 3, 4\}$ , and all seven it misses are matchings. (Only the empty one is a theorem here, Theorem 7.5; the other six are a measurement.)

**8.6. Controls.** Three of the controls on the elimination recursion are worth stating, because they refute the failure modes a negative computation can have. Dropping the pivot branch from the recursion reports the empty graph on  $\{1, 2, 5, 6, 11\}$  as unreachable, and dropping the  $G \star v$  branch reports the single edge  $\{6, 11\}$  as unreachable — yet Theorem 8.1 exhibits explicit words for both, so a truncated recursion would produce false negatives, exactly the error a blocking argument must not make. (Quantitatively, dropping either branch collapses the leaf count from 19 305 to 509 or 510 and the covered set from 1023 to 955 or 933.) On the subset  $\{0, 1, 2, 3, 4\}$  the recursion produces all 1024 targets, so it does not report spurious blocks. And the recursion is checked against the entirely different algorithm of Section 7 — linear algebra on the graph-state code, with no graph recursion in it — on all sixteen graphs where that algorithm has a verdict, namely  $C_5$ ,  $C_6$  (twice), the Petersen graph,  $P_{13}$  (twice), the eight graphs of Theorem 7.4 and two further order-13 controls: the two agree in all sixteen cases, with both verdicts occurring. With Theorem 7.6 the three algorithms now agree pairwise on the same sixteen graphs.

*Remark 8.5.* The following is a record of computation carried out outside the formal development, included so that the choice of  $G_{14}$  is auditable. The exact objective (5) was evaluated on all 1020 published extremal  $(14, 2^{14}, 6)$  Type II codes: every one of them has  $\text{def}_5 > 0$ , with values ranging from 12 to 7462 and median 68, and the minimum 12 is attained at exactly two of them,  $G_{14}$  and one other. Iterated local search on the exact objective from 25 seeds (21 488 exact evaluations, 2.4 CPU-hours) never went below 12; exhaustive single- and double-edge-toggle scans around the nine best graphs found 0 improvements in 15 676 feasible neighbours, including every single toggle in each of the 15 immediate local-complementation representatives of  $G_{14}$ . Total cost 3.35 CPU-hours. *No order-14 witness was found*, and this is a search record, not evidence that none exists. A complete sweep of order 14 is not available: the length-14 codes with  $d = 5$  have never been classified, and a length-14 graph with  $d \geq 5$  need not have a vertex whose deletion keeps  $d \geq 5$ , so the lengthening chain used at order 13 does not start.

9. VERTEX-MINOR UNIVERSALITY OVER  $\mathbb{F}_p$ 

**9.1. The operations.** A qudit graph state on  $n$  qudits of prime dimension  $p$  is described by a *label matrix*  $M \in \mathbb{F}_p^{n \times n}$ , symmetric with zero diagonal — equivalently, a complete graph on  $\{0, \dots, n-1\}$  whose edge  $\{j, k\}$  carries the label  $M_{jk}$ , an edge of label 0 being absent. Bahramgiri and Beigi [4] give two operations on such matrices. For  $v$  a vertex and  $a \in \mathbb{F}_p$ , the *generalised local complementation*  $M *_a v$  has entries

$$(6) \quad (M *_a v)_{jk} = M_{jk} + a M_{vj} M_{vk} \quad (j \neq k), \quad (M *_a v)_{jj} = 0;$$

and for  $b \in \mathbb{F}_p^\times$ , the *local scaling*  $M \circ_b v$  multiplies row  $v$  and column  $v$  by  $b$  and leaves every other entry alone. Row  $v$  is fixed by (6) automatically, since  $M_{vv} = 0$ . At  $p = 2$  and  $a = b = 1$ ,  $*_1 v$  is ordinary local complementation and  $\circ_1 v$  is the identity. Bahramgiri and Beigi prove that two qudit graph states are equivalent under the local Clifford group if and only if some sequence of these operations carries one label matrix to the other; that theorem is what licenses reading the orbit below as a local Clifford orbit, and nothing formally proved here depends on it. They also define vertex deletion  $d(v)M$  — zero every label at  $v$  — which we use in the same way as in the binary case.

*Remark 9.1.* The definition as printed in [4] — the unnumbered Definition preceding Theorem 5, in Section III.D, on p. 6 of v2 and p. 5 of v1 — carries two index defects, and they are present in both arXiv versions: the scaling is written with label matrix  $I(v, b) M I(b, a)$ , in which  $a$  is unbound and the intended right factor is  $I(v, b)$ ; and the operator named  $*_a w$  is given by  $M'_{jk} = M_{jk} + a M_{vj} M_{wk}$ , in which the intended index is  $w$ . Both are resolved by the same authors' companion paper [5], Definition 3.1 of v2, which states the two operations over a general finite field with consistent indices: there  $G *_r v$  fixes row  $v$  and sets  $g'_{uw} = g_{uw} + r g_{vu} g_{vw}$  for  $u, w \neq v$ , and  $G \circ_s v$  multiplies row and column  $v$  by  $s \neq 0$ . Equation (6) and the scaling above are that reading.

**9.2. Universality, and the quantity  $\nu_p$ .** A *move* is one of the  $2n(p-1)$  operations  $*_a v$ ,  $\circ_a v$  with  $a \in \{1, \dots, p-1\}$  and  $v < n$ ; a *word* is a finite sequence of moves, and  $M * w$  denotes their composite. For an ordered  $k$ -subset  $S$  we write  $M[S]$  for the induced label matrix.

**Definition 9.2.** A label matrix  $M$  of order  $n$  is  *$k$ -vertex-minor universal over  $\mathbb{F}_p$*  if  $k \leq n$  and for every  $k$ -subset  $S$  and every one of the  $p^{\binom{k}{2}}$  labelled  $\mathbb{F}_p$ -graphs  $F$  on  $S$  there is a word  $w$  with  $(M * w)[S] = F$ . We write  $\nu_p(k)$  for the least order of such a matrix.

This is Definition 1.1 with “graph” replaced by “ $\mathbb{F}_p$ -labelled graph” and  $\nu_2 = \nu$ . Targets are exact labelled matrices, not classes up to local scaling on  $S$ ; the coarser variant is a weaker requirement and would give values at most these. As before, the deletions may be postponed: a deletion outside  $S$  does not change  $M[S]$ , and this is proved in the formal development, so the orbit-then-restrict form of the definition is the one used throughout. We are not aware of any prior occurrence of Definition 9.2. Both ingredients are in print: the operations are [4], and Section 4 of [12] develops  $\mathbb{F}_q$ -labelled graphs with cut-rank over  $\mathbb{F}_q$  on the strength of [4], in a paper whose introduction cites the vertex-minor universality paper [8]; Chapter 3 of [10] carries the same  $\mathbb{F}_q$ -labelled material and Chapter 7 the universality, for qubits only. We could not find them combined anywhere, and this should be read as “not found” rather than as “new”.

**Proposition 9.3.** *The two operations preserve well-formedness (symmetric, zero diagonal, entries below  $p$ ), and the two certificate shapes of Section 3 carry over verbatim with  $2^{\binom{k}{2}}$  replaced by  $p^{\binom{k}{2}}$  and the  $n$  local complementations replaced by the  $2n(p-1)$  moves: a verified covering family proves  $k$ -vertex-minor universality, and a verified blocking certificate at order  $n$  proves that no label matrix of order  $n$  decoded from a code is  $k$ -vertex-minor universal.*

**Proposition 9.4.** *For all  $p \geq 1$  and all  $n$ , the base- $p$  decoding map  $c \mapsto$  (label matrix with code  $c$ ) is onto the  $\mathbb{F}_p$  label matrices of order  $n$ , and is a left inverse of the encoding. Consequently a blocking certificate at order  $n$  proves that every  $\mathbb{F}_p$  label matrix of order  $n$  fails to be  $k$ -vertex-minor universal, not merely every decoded code.*

*Proof sketch.* The code of the matrix induced on an ordered list  $S$  splits as the code of the tail plus a base- $p$  numeral whose digit  $i$  is the label from the head of  $S$  to  $S_i$ ; digit extraction then follows by induction on  $S$ , using the triangular recurrence for the pair positions to bound the low digits. The proof is uniform in  $p$  and  $n$  and uses no computation. This is bookkeeping rather than mathematics, but it is what makes each lower bound below a statement about all label matrices.  $\square$

### 9.3. $k = 2$ , uniformly in $p$ .

**Theorem 9.5.** *Let  $p \geq 2$  be such that  $\mathbb{F}_p$  has no zero divisors. Then  $\nu_p(2) = 3$ . Precisely: the triangle  $K_3^{(1)}$  on  $\{0, 1, 2\}$  with all three labels equal to 1 is 2-vertex-minor universal over  $\mathbb{F}_p$ , and no  $\mathbb{F}_p$  label matrix on two vertices is.*

*Proof. Upper bound.* Let  $S = \{a, b\}$  and let  $c$  be the third vertex. If the target label is  $m \neq 0$ , then  $K_3^{(1)} \circ_m a$  has label  $1 \cdot m = m$  on  $\{a, b\}$ . If the target label is 0, then  $K_3^{(1)} *_{p-1} c$  has label  $1 + (p-1) \cdot 1 \cdot 1 = p \equiv 0$  on  $\{a, b\}$ . Three pairs times these two cases: every cell is realised by a word of length one.

*Lower bound.* Let  $n = 2$ , so that the matrix is determined by the single label  $M_{01}$ . For either vertex  $u$  and any  $a$ , the term  $a M_{uj} M_{uk}$  that  $*_a u$  adds to  $M_{jk}$  with  $\{j, k\} = \{0, 1\}$  has  $u \in \{j, k\}$ , hence a factor  $M_{uu} = 0$ ; so  $*_a u$  is the identity on two vertices. The only other moves are the scalings  $\circ_b u$ , which multiply  $M_{01}$  by  $b \neq 0$ . Because  $\mathbb{F}_p$  has no zero divisors,  $b M_{01} = 0$  if and only if  $M_{01} = 0$ , so the predicate “ $M_{01} = 0$ ” is invariant along every word. Whichever value it takes at  $M$ , one of the two targets 0 and 1 on  $\{0, 1\}$  is unreachable. Finally  $n < 2$  is excluded because  $k \leq n$  is part of Definition 9.2.  $\square$

Three remarks. First, no computation occurs anywhere in this proof, and the statement is uniform: it covers every prime, including all those no exhaustive search will reach. Second, the hypothesis in the formal development is not primality but the bounded arithmetic condition “ $xy \equiv 0 \pmod{p}$  with  $x, y < p$  implies  $x = 0$  or  $y = 0$ ”, which for  $p \geq 2$  is equivalent to it; that condition is checked to hold at  $p = 2, 3, 5, 7$  and to fail at  $p = 4, 6, 9$ , so it is a real restriction and not decoration. Third, at  $p = 2$  the theorem specialises to the published statement that  $K_3$  is the smallest 2-vertex-minor universal graph [11], and the specialisation is itself part of the formal development; the theorem is therefore not a claim about the qubit value.

### 9.4. $k = 3$ and $k = 4$ , by certificate.

**Theorem 9.6.**  $\nu_3(3) = 6$ . *The witness is  $C_6^{(1)}$ , the 6-cycle with every label 1; and no  $\mathbb{F}_3$  label matrix of order 3, 4 or 5 is 3-vertex-minor universal.*

**Theorem 9.7.**  $6 \leq \nu_3(4) \leq 10$ . *The upper bound is witnessed by the Petersen graph with every label 1, which is 4-vertex-minor universal over  $\mathbb{F}_3$ ; and no  $\mathbb{F}_3$  label matrix of order 4 or 5 is 4-vertex-minor universal.*

**Theorem 9.8.**  $5 \leq \nu_5(3) \leq 6$ . *The upper bound is witnessed by the same all-ones 6-cycle  $C_6^{(1)}$ , now over  $\mathbb{F}_5$ ; and no  $\mathbb{F}_5$  label matrix of order 3 or 4 is 3-vertex-minor universal.*

*Proof sketch for Theorems 9.6–9.8.* Every upper bound is a covering family in the sense of Proposition 9.3, verified against every cell:

| witness                                     | field          | cells                                | words | alphabet |
|---------------------------------------------|----------------|--------------------------------------|-------|----------|
| $C_6^{(1)}$ , order 6, $k = 3$              | $\mathbb{F}_3$ | $\binom{6}{3} \cdot 3^3 = 540$       | 267   | 24 moves |
| $C_6^{(1)}$ , order 6, $k = 3$              | $\mathbb{F}_5$ | $\binom{6}{3} \cdot 5^3 = 2500$      | 672   | 48 moves |
| Petersen <sup>(1)</sup> , order 10, $k = 4$ | $\mathbb{F}_3$ | $\binom{10}{4} \cdot 3^6 = 153\,090$ | 7942  | 40 moves |

The  $\mathbb{F}_3$  words for  $C_6^{(1)}$  have length at most 4 and were found by a breadth-first search of its entire local-equivalence orbit (86 688 label matrices, under a second); the Petersen words have length at most 45 and were found by random walk. That the landed order-10 matrix really is the Petersen graph —

outer 5-cycle, inner pentagram, five spokes — is itself verified, so the witness is pinned to the named graph.

Every lower bound is a blocking certificate, exhaustive over all label matrices of the order in question by Proposition 9.4: at  $p = 3$  over the  $3^3 = 27$ ,  $3^6 = 729$  and  $3^{10} = 59\,049$  matrices of orders 3, 4, 5 (for  $k = 3$ ) and the last two (for  $k = 4$ ); at  $p = 5$  over the  $5^3 = 125$  and  $5^6 = 15\,625$  matrices of orders 3 and 4. Each certificate is checked for invariance under every one of the  $2n(p-1)$  moves at every code and for non-realisation of its own cell, and it re-checks that the encoding is injective at every code, so the enumeration misses nothing. Orders below  $k$  need no certificate, since  $k \leq n$  is part of Definition 9.2.  $\square$

*Remark 9.9.* Both brackets are closed outside the formal development, by the same certificate search run in C rather than in the kernel. At  $p = 5$ , all  $5^{10} = 9\,765\,625$  label matrices of order 5 fall into 145 local-equivalence orbits and none is 3-vertex-minor universal (59 seconds), so  $\nu_5(3) = 6$ . At  $p = 3$ , all  $3^{15} = 14\,348\,907$  label matrices of order 6 fall into 1241 orbits and none is 4-vertex-minor universal (100 seconds), so  $\nu_3(4) \geq 7$ . Neither is a theorem here: reproducing them in the kernel costs, at the measured rate of the certificates that were run — about  $9.6 \cdot 10^3$  (code, move) pairs per second at order 5, and about half that per pair at order 6 — some 11 and 19 CPU-hours respectively, plus blocking tables of 19.5 and 43 megabytes (two and three bytes per code). A fourfold saving is available at  $p = 5$  and a twofold one at  $p = 3$  by shrinking the move alphabet from  $2n(p-1)$  to  $2n$ , using  $*_a v = (*_1 v)^a$  and  $\circ_b v = (\circ_g v)^i$  for  $g$  a primitive root; that would bring the first inside a four-hour budget and not the second, and it is not done here.

## 9.5. Controls.

**Proposition 9.10** (controls). *Inside the formal development: at  $p = 2$  the general statement of Theorem 9.5 returns the published value  $\nu(2) = 3$  with no computation, and the certificate route returns the published value  $\nu(3) = 6$ , from blocking certificates at orders 3, 4, 5 over the 8, 64 and 1024 binary label matrices together with a 61-word covering family for the same all-ones 6-cycle. Over all 1024 labelled graphs of order 5 the  $\mathbb{F}_p$  encoding agrees with the binary one of Section 2.2: the decoders agree, the induced codes agree on all ten 3-subsets, and the move  $*_1 u$  is exactly local complementation at  $u$  while  $\circ_1 u$  is the identity. Both generators are invertible on all 729 order-4 qutrit matrices. The certificate checker rejects an empty family, a family with its last word removed, and a family offered at the wrong  $k$ ; the blocking checker rejects an all-zero table, a table with an out-of-range cell, and a table whose invariance fails at one code. Finally, no sequence of generalised local complementations and local scalings makes the qutrit  $C_5^{(1)}$  induce the empty labelled matrix on  $\{0, 1, 2\}$ .*

The last item is Claudet’s own justification for “no graph of order 5 is 3-vertex-minor universal” — exploring the 132-element orbit of  $C_5$  and finding no independent triple — transported one prime up and stated for every word rather than by orbit enumeration; the blocked cell was read out of the certificate rather than chosen. One further check is outside the formal development but is the strongest single test that (6) and the scaling are transcribed correctly: an independently written re-implementation, sharing no code with the search program, partitions the connected  $\mathbb{F}_3$  label matrices of orders 3, 4 and 5 into local-equivalence orbits and counts isomorphism classes per orbit, obtaining 7 at order 3; 10, 37, 6 at order 4; and 11, 88, 255, 219, 139 at order 5 — exactly the corresponding entries of the column  $|V|$  of Table 1 of the qutrit orbit classification [21], all five order-5 values included.

## 9.6. The table, and a question.

|            | $p = 2$ | $p = 3$           | $p = 5$       | $p = 7$ |
|------------|---------|-------------------|---------------|---------|
| $\nu_p(2)$ | 3       | 3                 | 3             | 3       |
| $\nu_p(3)$ | 6       | 6                 | $[5, 6]; = 6$ | $= 6$   |
| $\nu_p(4)$ | 10      | $[6, 10]; \geq 7$ | —             | —       |

The whole first row is Theorem 9.5, one statement covering every prime. The  $p = 2$  column is published [11, 10] and is reproduced here as a control, not claimed. Brackets are the theorems of Section 9; an entry after a semicolon is the value or bound obtained outside the formal development,

by the certificate search run in C (Remark 9.9). The entry  $\nu_7(3) = 6$  is of that second kind throughout: orders 3 and 4 are blocked, the all-ones 6-cycle is 3-vertex-minor universal over  $\mathbb{F}_7$  with a 1844-word covering family, and all  $7^{10} = 282\,475\,249$  label matrices of order 5 fall into 189 orbits, none of them universal (58 minutes, 2.2 gigabytes). No statement in this paper rests on it.

Two regularities stand out, and neither is explained here. Every determined entry agrees across the four primes; at  $k = 3$  the witness is literally the same matrix at  $p = 2, 3, 5$  — one array, three certificates — and the same 6-cycle again at  $p = 7$ ; and at  $k = 4$  it is the same graph at  $p = 2, 3$ . That is a stronger coincidence than equality of the minimal orders.

**Question 9.11.** Is  $\nu_p(k)$  independent of  $p$ ?

The cheapest genuine test is the qutrit  $k = 4$  cell, which is decided by orders 7, 8 and 9. Exhaustive search there is out of reach ( $3^{21} \approx 1.05 \cdot 10^{10}$  label matrices at order 7 alone), but a *positive* answer at any of those orders would settle Question 9.11 in the negative outright, and a covering family needs no exhaustive search. Random-walk probes have not found one: at order 7, the best of 265 random candidates covered 24 724 of the 25 515 cells; at order 9, the best of 73 covered 91 747 of 91 854, and a walk fifty times longer on that candidate saturates at exactly the same number, so those 107 cells are a genuine obstruction for that matrix rather than under-sampling. This is a search record and not evidence of a bound.

*Remark 9.12.* The literature contains a second, smaller group: the  $\lambda$ -local complementations of [18] act by (6) alone, with no local scaling, so “locally equivalent” there is a finer relation than local Clifford equivalence. The two differ — over  $\mathbb{F}_3$  the numbers of orbits at orders 3, 4, 5 are 8, 39, 199 for the star-only group against 5, 19, 109 for the full group — but at the cells above they give the same answers:  $\nu_p(2) = 3$  at  $p = 3, 5$  and no 3-vertex-minor universal  $\mathbb{F}_3$  matrix of order at most 5. So none of the values in this section is an artefact of which group is taken. This comparison was made outside the formal development.

## 10. VERIFICATION

Every theorem and proposition of this paper — with the single exception of Lemma 8.3, which is quoted from the literature and is flagged at each use — has been formally verified in Lean 4 (toolchain v4.32.0); the development is free of `sorry`, and it deliberately imports no library beyond Lean’s own prelude — no Mathlib — so that the finite checks run on flat machine-integer and array code. The reasoning layer is kernel-only, using no compiled evaluation at all: the two bridges of Proposition 3.1, the encoding facts of Propositions 3.2 and 9.4, the whole of Section 6 (Proposition 6.1 and Theorem 6.2), the corresponding  $\mathbb{F}_p$  layer of Proposition 9.3, and Theorem 9.5 in its entirety depend on no axioms beyond `propext`, `Classical.choice` and `Quot.sound`. What is delegated to compiled evaluation, through Lean’s `native_decide`, is exactly the finite searches, and each theorem names the single evaluation it rests on: one covering-family check per positive result; one blocking-certificate check per exhaustive negative statement, over the 2, 8, 64, 1024 and 32768 labelled graphs of orders 2 to 6 at  $p = 2$  and over the label-matrix counts tabulated in Section 9 at  $p = 3, 5$ ; one line search per graph in Theorem 7.4; one elimination-tree evaluation per subset in Theorem 8.4; one criterion evaluation per cell in Theorems 7.5, 7.6 and 8.2; and one identity comparison per order in Proposition 7.1. Every numerical value quoted was first produced by an independent implementation in C, and the formal statement was then written against it: the twelve cells of Table 1 agree, cell for cell, across three implementations — an optimised C search with dynamic elimination order, transposition table and component pruning; a C computation of the reachable set from the code side, sharing no algorithm with it; and the formal development itself — and the graph codes of two of the  $k = 4$  witnesses are re-derived inside the development from the values printed by the C search program, so the certificates were not checked in a different convention from the one that produced them. The whole development checks in about one hour of CPU time on a single core. Repository reference to be added at submission.

## REFERENCES

- [1] J. C. Adcock, S. Morley-Short, A. Dahlberg, J. W. Silverstone, *Mapping graph state orbits under local complementation*, Quantum **4** (2020) 305, doi:10.22331/q-2020-08-07-305, arXiv:1910.03969.
- [2] R. Ascoli, B. Frederickson, S. Frederickson, C. McFarland, L. Post, *Almost all graphs are vertex-minor universal*, arXiv:2602.09049 (February 2026).
- [3] J. H. Bae, *Vertex-minor Ramsey numbers: exact values and extremal structure*, arXiv:2604.13434 (April 2026).
- [4] M. Bahramgiri, S. Beigi, *Graph states under the action of local Clifford group in non-binary case*, arXiv:quant-ph/0610267 (v1 October 2006, v2 June 2007); no journal version.
- [5] M. Bahramgiri, S. Beigi, *Enumerating the classes of local equivalency in graphs*, arXiv:math/0702267 (v1 February 2007, v2 July 2007); no journal version.
- [6] A. Bouchet, *Graphic presentations of isotropic systems*, J. Combin. Theory Ser. B **45** (1988) 58–76, doi:10.1016/0095-8956(88)90055-X.
- [7] S. Bravyi, Y. Sharma, M. Szegedy, R. de Wolf, *Generating  $k$  EPR-pairs from an  $n$ -party resource state*, Quantum **8** (2024) 1348, doi:10.22331/q-2024-05-14-1348, arXiv:2211.06497.
- [8] M. Cautrès, N. Claudet, M. Mhalla, S. Perdrix, V. Savin, S. Thomassé, *Vertex-minor universal graphs for generating entangled quantum subsystems*, ICALP 2024, LIPIcs **297**, article 36, pp. 36:1–36:18, doi:10.4230/LIPIcs.ICALP.2024.36, arXiv:2402.06260.
- [9] T.-W. Chao, Z. Xu, *Vertex-minor universality of a random graph*, arXiv:2603.13600 (March 2026).
- [10] N. Claudet, *Local Equivalences of Graph States*, PhD thesis, Université de Lorraine, defended 17 November 2025; arXiv:2511.22271, Chapter 7 (“Vertex-minor universal graphs”); that chapter is unchanged between v1 and v2.
- [11] N. Claudet, M. Mhalla, S. Perdrix, *Small  $k$ -pairable states*, arXiv:2309.09956v2 (October 2023); the relevant items are its Table 1 and its Section 5.
- [12] N. Claudet, S. Perdrix, *Covering a graph with minimal local sets*, in: Graph-Theoretic Concepts in Computer Science (WG 2024), Lecture Notes in Computer Science **14760**, Springer, 2025, pp. 136–150, doi:10.1007/978-3-031-75409-8\_10; arXiv:2402.10678. Section 4 of the arXiv version develops  $q$ -multigraphs with cut-rank over  $\mathbb{F}_q$ .
- [13] L. E. Danielsen, *Graph-based classification of self-dual additive codes over finite fields*, Adv. Math. Commun. **3** (2009), no. 4, 329–348, doi:10.3934/amc.2009.3.329, arXiv:0801.3773.
- [14] L. E. Danielsen, 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, doi:10.1016/j.jcta.2005.12.004, arXiv:math/0504522.
- [15] L. E. Danielsen, *Database of Self-Dual Quantum Codes*, the local-complementation orbit data accompanying [14], now hosted at [codetables.de/larsed/vncorbits/](https://codetables.de/larsed/vncorbits/) (all orbits for length at most 12; for length 14, extremal Type II codes only). The original University of Bergen pages that held this data are no longer reachable, so this is the only live copy; the host site, *Code Tables: Bounds on the parameters of various types of codes* ([codetables.de](https://codetables.de)), is maintained by M. Grassl.
- [16] D. G. Fon-Der-Flaass, *On local complementations of graphs*, in: Combinatorics (Eger, 1987), Colloq. Math. Soc. János Bolyai **52**, North-Holland, Amsterdam, 1988, pp. 257–266; Zbl 0728.05048.
- [17] D. Kim, S. Oum, *Vertex-minors of graphs: a survey*, Discrete Appl. Math. **351** (2024) 54–73, doi:10.1016/j.dam.2024.03.011.
- [18] A. Marin, D. Markham, S. Perdrix, *Access structure in graphs in high dimension and application to secret sharing*, TQC 2013, LIPIcs **22**, pp. 308–324, doi:10.4230/LIPIcs.TQC.2013.308, arXiv:1304.7105.
- [19] M. Van den Nest, J. Dehaene, B. De Moor, *Graphical description of the action of local Clifford transformations on graph states*, Phys. Rev. A **69** (2004) 022316, doi:10.1103/PhysRevA.69.022316, arXiv:quant-ph/0308151.
- [20] OEIS Foundation Inc., *The On-Line Encyclopedia of Integer Sequences*, <https://oeis.org>; entry A016729 (highest minimum distance of a Hermitian self-dual additive  $GF(4)$  code of length  $n$ ).
- [21] K.-R. Revis, H. Zakaryan, Z. Raissi, *Orbit classification and analysis of qutrit graph states under local complementation and local scaling*, arXiv:2506.05478v1 (June 2025); the orbit data used here is the column  $|V|$  of its Table 1.
- [22] Z. Varbanov, *Some new Results for Additive Self-Dual Codes over  $GF(4)$* , Serdica J. Computing **1** (2007), no. 2, 213–227; Zbl 1221.94084.