Deterministic quadratic-size graphs for labelled vertex-minors

Yuxuan Zhang[1,2]
[1]École Polytechnique Fédérale de Lausanne
[2]Princeton University

27 November 2026 · Version 1.0

Abstract

A graph is k-vertex-minor universal if every graph on every specified set of k of its vertices can be obtained by local complementations and deletions. We give a deterministic polynomial-time construction on $O(k^2)$ vertices. The construction combines a strong subspace design with an average-rank bound for field traces. Each group of switches programs a quadratic edge pattern. Private error-correcting coordinates allow even the switches and their hubs to be prescribed as outputs. Fourier inversion establishes the existence of the required sequence for each target.

1 The construction problem

Local complementation at v complements the graph induced by its neighbors and leaves its incident edges in place. Deletion removes one vertex and all of its incident edges. In both operations each surviving vertex keeps its label.

Theorem 1. *There are an absolute constant C and a deterministic algorithm which, on unary $k \geq 2$, outputs in $k^{O(1)}$ time a finite simple graph G on between k and Ck^2 vertices. For every k-subset S of its vertices and every simple graph H on S, H is a vertex-minor of G on precisely those labels.*

Cautrès et al. proved quadratic existence, gave explicit quartic-size incidence graphs, and asked for a deterministic construction of cubic or quadratic order [1]. Ascoli et al. and Chao and Xu proved further random-graph guarantees [2, 3]. The catalogue formulation asks about the time to generate a labelled graph. Theorem 1 concerns the time to produce the resource graph. Finding the local operations for a particular target in polynomial time remains a separate algorithmic question.

The construction is bipartite. One side contains data vertices and hubs. The other consists of switches, each joined to precisely its own hub and to a specified set of data vertices. The first step provides the binary maps that determine these sets.

2 A short list of projections

Let Q be the least power of two at least $2^{20}k^2$, let $m_0 = \log_2 Q$, and put $s = km_0$. All choices below can use lexicographically first representatives in fixed polynomial bases.

Lemma 2. *For all sufficiently large k there is a deterministic polynomial-time list of B binary $32k$-by-s matrices with $100k \le B \le 101k$. For every binary s-by-r matrix U of column rank $r \le k$,*

$$\frac{1}{B}\sum_{b}(r - \operatorname{rank} M_b U) \le 0.30r.$$

Proof. Choose the least power q of four with $q^3 \ge 2s$. Set $m = q^3 - 1$, so $s \le m < 128s$. We first build $D = \lceil 1600s/k \rceil$ maps $E_i : \mathbb{F}_q^s \to \mathbb{F}_q^{16k}$. For every r-space V in the domain they satisfy

$$\sum_i \dim(V \cap \ker E_i) \le \frac{4mr}{8(2k - r + 1)}. \tag{1}$$

Here are the details needed from the cyclotomic subspace design of Guruswami, Xing and Yuan [4]. They also explain the choice of auxiliary field and the number of available evaluations. Use a primitive cubic conductor over $\mathbb{F}_q$ in their Sections 2–4. The cyclotomic function field $F/\mathbb{F}_q(x)$ is cyclic of degree m with generator σ and genus $g = O(m)$. The genus formula there gives $g \le m + 1$. Their Lemma 2.5 computes an m-dimensional space complementary to $\mathcal{L}(\mathcal{D} - Q')$ in $\mathcal{L}(\mathcal{D})$, where Q' lies over the rational zero of x. The invariant divisor $\mathcal{D}$ has degree $3\lceil (2g + m - 1)/3 \rceil \le 4m$ for large m. Restrict to the first s basis functions. By their Lemmas 3.1 and 3.3, any r vectors independent over $\mathbb{F}_q$ give a nonzero Moore determinant with rows of consecutive σ-conjugates. Its pole degree is at most $r \deg \mathcal{D}$.

Take disjoint blocks of $t = 2k$ consecutive conjugate places of degree eight from split orbits. The map E_i evaluates the linear combination of basis functions at the t places, giving $8t = 16k$ coordinates. If a basis vectors of V vanish on a block, choose them as the first a columns in the Moore determinant. At each of $t - r + 1$ consecutive places in the block these columns vanish, using the orbit order consistent with σ. Thus the determinant has zero degree at least $8a(t - r + 1)$ on that block. A constant change of basis only scales the determinant. Summing over the disjoint blocks proves (1).

For clarity, only completely split degree-eight base places are used. The number of degree-eight places upstairs is at least

$$(q^8 - q^4 - 2g(q^4 + q^2))/8$$

by subtracting the $\mathbb{F}_{q^4}$ points from the $\mathbb{F}_{q^8}$ points and applying the curve point bound. For q large this is $\Omega(q^8)$, since $g = O(q^3)$. Omit places above the conductor and infinity, at most $O(m)$. At any remaining degree-eight place the residue degree divides both eight and the odd extension degree m. It equals one, so the underlying degree-eight place splits completely. Each orbit of length m yields $\lfloor m/t \rfloor$ disjoint blocks. For large k, $m \ge 2t$, giving $\Omega(q^8/t)$ blocks, more than D. At fixed conductor and place degrees the defining polynomials, roots in $\mathbb{F}_{q^8}$, and conjugates can be enumerated in polynomial time. Basis computation and evaluation use Lemmas 2.4–2.5 of [4]. This count and algorithm only use the blocks actually found. From (1), the mean rank loss on the first D blocks is at most $r/20$.

A binary matrix has the same rank after scalar extension to $\mathbb{F}_q$. For each E_i and each $\alpha \in \mathbb{F}_q$ apply the relative trace $\operatorname{Tr}_{q/4}(\alpha \cdot)$ to every output, and expand each $\mathbb{F}_4$ coordinate into two bits. This gives a binary linear map on binary inputs. If $h = \operatorname{rank} E_i U > 0$, choose a nonsingular h-minor V and write $q = 4^a$. The polynomial

$$d(z) = \det\left(\sum_{j=0}^{a-1} z^{4^j} V^{(4^j)}\right)$$

has degree $hq/4$ and leading coefficient $(\det V)^{q/4}$. Here a parenthesized power acts entrywise. At $z = \alpha$ the nullity of the matrix is at most the multiplicity of the root: constant row operations put that many rows in $(z-\alpha)\mathbb{F}_q[z]^h$. Averaging nullity over the q choices thus loses at most $h/4$. Binary expansion on binary inputs preserves at least the $\mathbb{F}_4$ rank of the traced minor. Including $h = 0$, total mean deficiency is at most $(1/20 + 1/4)r$. Finally $Dq = O((k \log k)^{1/3} \log k) = o(k)$. Repeat the whole list equally often, taking the least multiple B of Dq at least $100k$. □

3 Switches and protected outputs

Index the data by $x \in \mathbb{F}_Q^\times$. Their prefixes $c_x \in \mathbb{F}_2^s$ are the binary coordinates of $(x, x^3, \dots, x^{2k-1})$. Any at most k distinct prefixes are independent. Indeed a zero binary sum on the odd powers gives zero sums on every power from one through k by squaring. For j selected points the matrix of powers $1, \dots, j$ is a Vandermonde matrix times an invertible diagonal.

A nonzero functional on the prefixes has weight at least

$$(Q - (2k-2)\sqrt{Q})/2. \tag{2}$$

By nondegeneracy of the field trace it is $x \mapsto \mathrm{Tr}_{Q/2}\, f(x)$ for a polynomial with odd exponents and nonzero leading coefficient of odd degree $d \le 2k-1$. The additive character sum has magnitude at most $(d-1)\sqrt{Q}$; equivalently, apply the curve point bound to $y^2 + y = f(x)$, of genus $(d-1)/2$ with one point at infinity. This is the classical dual BCH weight bound [5]. The zero coordinate has value zero.

Each bank b has one hub and $32k$ switches. Switch j is joined to its hub and has raw incidence bit $(M_b c_x)_j$ at x. Choose disjoint private data groups of size L for all banks. On its private group, a bank adds modulo two the corresponding rows of an injective binary length-L code with $32k$ message bits and distance $> k$.

For an explicit code put $h = \lceil \log_2(64k) \rceil$ and $K = \lceil 32k/h \rceil$. Pad to Kh message bits and use a Reed–Solomon evaluation code of length $2K$ and dimension K over $\mathbb{F}_{2^h}$. Encode each symbol by a binary linear code of dimension h, length $8h$, and distance at least h. It can be built greedily: before each extension fewer than $2^h \sum_{i<h} \binom{8h}{i} < 2^{8h}$ vectors are forbidden, by the binary entropy bound. Enumeration costs $2^{O(h)}$. Thus $L = 16Kh \le 528k$ for $h \le k$, and the distance is at least $(K+1)h$. Our choice of Q pays both for BL private coordinates and for (2) to exceed $kL + k$.

Lemma 3. *Any at most k switch columns are linearly independent on the data remaining after any at most k data deletions.*

Proof. Consider a nonempty sum of selected columns. Its raw incidence word is a functional on c_x. If the functional is nonzero, (2) exceeds the combined damage from k private groups and k deletions. If it is zero, an occupied bank contributes a nonzero private codeword of weight $> k$, on coordinates disjoint from all other private groups. □

4 Programming the graph on prescribed labels

Partition the prescribed terminals into data P, switches L_0 and hubs H. For each named hub reserve one extra, nonterminal switch in its bank. Let Y consist of L_0 and these bonus switches. By Lemma 3, choose $|Y|$ proxy data outside P with an invertible incidence matrix to Y. Write T for P together with those proxies, so $|T| = k$. Delete all other data. Exclude banks containing a

prescribed switch or hub and banks with private data in T. There are at most $2k$ excluded banks. In them keep precisely the designated hubs and the switches in Y.

For every remaining bank, complement at selected switches and delete all of its switches. Its hub now has neighborhood vector $v = C_T^\top M_b^\top z$ on T, where C_T has the prefixes as columns and z lists the selected switches. The switches were independent vertices, so their other effect is a sum of fixed cliques, linear in z. Complement at the hub and delete it. The total added pattern on T is $q(v) + L_b(z)$, where $q(v)_{ij} = v_i v_j$ for $i < j$ and L_b is linear. Other banks and the retained switch incidences are unaffected.

Test the sum of these patterns against the character given by a nonzero alternating binary matrix A of rank r. Factor it as $WJW^\top$ with W of column rank r and J the fixed nonsingular alternating matrix of order r. Set $U = C_T W$, also of rank r. In bank b the polar matrix on selector bits is $M_b U J U^\top M_b^\top$. Its rank is at least $2\,\mathrm{rank}(M_b U) - r$ by the product rank inequality. Lemma 2 gives a total of at least $0.40Br$ over all banks. Removing the excluded banks costs at most $2kr$, leaving at least $38kr$.

For uniform independent selector bits a quadratic polynomial of polar rank a has absolute bias at most $2^{-a/2}$, regardless of its linear part. Squaring the character average and differencing in the input shows that only shifts in the polar kernel contribute. Hence the bias for our character over all available banks is at most 2^{-19kr}. There are at most 2^{kr} alternating matrices of rank r by the displayed factorization. After normalization the sum of all nontrivial absolute Fourier coefficients is bounded by $\sum_{r=2}^{k} 2^{-18kr} < 1$. Fourier inversion gives positive mass to each edge pattern on T. These random variables count choices in one fixed graph.

5 Returning each output to its original vertex

Use the graph-state phase convention $(-1)^{\sum_{i<j} a_{ij} x_i x_j}$. Write x for data in P, z for proxies, h for named hubs and $y = (l, b)$ for named and bonus switches, respectively. For any programmed quadratic q_0 on T, the remaining exponent is

$$q_0(x, z) + x^\top B_0 y + z^\top D_0 y + h^\top (E_0 l + b),$$

where D_0 is invertible. Measure the proxies and bonus switches in X and apply Hadamards to the named switches. In the zero-outcome branch Fourier summation over the old y imposes

$$D_0^\top z = B_0^\top x + (\ell + E_0^\top h,\, h).$$

Here ℓ is the new bit on the *same* named switch. This equation gives an invertible linear change between (x, ℓ, h) and (x, z). Arbitrary binary quadratic forms with zero constant term are closed under invertible linear substitution modulo linear terms. Thus every requested set of edge coefficients occurs on the prescribed labels, with linear phases removable by local Z operators. Other measurement outcomes add an affine translation and linear phases. Empty types obey the same argument with empty matrices.

Local Pauli measurements on deleted graph-state vertices give the usual labelled deletion rules up to local Cliffords; local Clifford equivalence of graph states is generated by local complementations [1, 6]. The computation uses only measurements on *discarded* vertices, including when the target contains isolated vertices. This proves labelled vertex-minor universality.

Finally, field choices, the size and distance inequalities, and the supply of evaluation blocks can all be tested during graph generation. Use the construction above when these tests hold, including $m \geq 16k$, $h \leq k$ and $Dq \leq k$. Otherwise use the explicit incidence graph of [1, Thm. 19] for the

least power of two at least $2k^2$. This branch is reached for only finitely many k and its order is then bounded by another absolute multiple of k^2. All operations in either branch take polynomial time, including writing the adjacency table. This finishes the proof of Theorem 1.

Verification. The supplement exhausts all 4,096 three-data, three-switch incidence/selection cases for one bank and tests the trace compression and the transfer of terminal labels separately. The asymptotic rank estimate and the supply of places use the arguments above. This preprint has received internal proof review. Independent specialist review and priority are open.

References

[1] M. Cautrès, N. Claudet, M. Mhalla, S. Perdrix, V. Savin and S. Thomassé, *Vertex-Minor Universal Graphs for Generating Entangled Quantum Subsystems*, ICALP 2024, 36. Conference paper; full version.

[2] R. Ascoli, B. Frederickson, S. Frederickson, C. McFarland and L. Post, *Almost All Graphs Are Vertex-Minor Universal*, RANDOM 2026, 38. Conference paper.

[3] T.-W. Chao and Z. Xu, *Vertex-Minor Universality of a Random Graph* (2026). arXiv:2603.13600.

[4] V. Guruswami, C. Xing and C. Yuan, *Subspace designs based on algebraic function fields*, Trans. Amer. Math. Soc. **370** (2018). Journal; full version and lemma numbering.

[5] J. F. Voloch, *On the duals of binary BCH codes*. Author's manuscript.

[6] A. Dahlberg, J. Helsen and S. Wehner, *How to transform graph states using single-qubit operations: computational complexity and algorithms*, Quantum Sci. Technol. **5** (2020), 045016. arXiv:1805.05306.