Vertex-Minor Universal Graphs for Generating Entangled Quantum Subsystems

Maxime Cautrès, Nathan Claudet, Mehdi Mhalla, Simon Perdrix, Valentin Savin, Stéphan Thomassé

Vertex-Minor Universal Graphs for Generating Entangled Quantum Subsystems

Maxime Cautrès
Université Grenoble Alpes, CEA-Léti, F-38054 Grenoble, France
École Normale Supérieure de Lyon, F-69007 Lyon, France

Nathan Claudet
Inria Mocqua, LORIA, CNRS, Université de Lorraine, F-54000 Nancy, France

Mehdi Mhalla
Université Grenoble Alpes, CNRS, Grenoble INP, LIG, F-38000 Grenoble, France

Simon Perdrix
Inria Mocqua, LORIA, CNRS, Université de Lorraine, F-54000 Nancy, France

Valentin Savin
Université Grenoble Alpes, CEA-Léti, F-38054 Grenoble, France

Stéphan Thomassé
Université de Lyon, École Normale Supérieure de Lyon, UCBL, CNRS, LIP, F-69007 Lyon, France

Abstract

We study the notion of k-stabilizer universal quantum state, that is, an n-qubit quantum state, such that it is possible to induce any stabilizer state on any k qubits, by using only local operations and classical communications. These states generalize the notion of k-pairable states introduced by Bravyi et al., and can be studied from a combinatorial perspective using graph states and k-vertex-minor universal graphs. First, we demonstrate the existence of k-stabilizer universal graph states that are optimal in size with $n = \Theta(k^2)$ qubits. We also provide parameters for which a random graph state on $\Theta(k^2)$ qubits is k-stabilizer universal with high probability. Our second contribution consists of two explicit constructions of k-stabilizer universal graph states on $n = O(k^4)$ qubits. Both rely upon the incidence graph of the projective plane over a finite field $\mathbb{F}_q$. This provides a major improvement over the previously known explicit construction of k-pairable graph states with $n = O(2^{3k})$, bringing forth a new and potentially powerful family of multipartite quantum resources.

2012 ACM Subject Classification Theory of computation → Quantum information theory; Theory of computation → Quantum communication complexity; Mathematics of computing → Graph theory

Keywords and phrases Quantum networks, graph states, vertex-minors, k-pairability

Digital Object Identifier 10.4230/LIPIcs.ICALP.2024.36

Category Track A: Algorithms, Complexity and Games

Related Version *Full Version*: `https://arxiv.org/abs/2402.06260` [3]
This work is a follow up of a previous arXiv preprint: `https://arxiv.org/abs/2309.09956` [6]

Funding This work was supported by the PEPR integrated project EPiQ ANR-22-PETQ-0007 part of Plan France 2030, by the STIC-AmSud project Qapla' 21-STIC-10, by the QuantERA grant EQUIP ANR-22-QUA2-0005-01, and by the European projects NEASQC and HPCQS.

1 Introduction

Quantum communication networks often rely on classical communication along with pre-shared entanglement. In this context, a highly pertinent problem is to explore which resource states enable a group of n parties, equipped with the capability of employing Local Operations and Classical Communication (LOCC), to create entangled EPR pairs among any k pairs

of qubits. It is only recently that Bravyi et al. addressed this fundamental question and provided both upper and lower bounds for what they called the k-pairability of quantum states, in terms of the number of parties and the number of qubits per party needed for a quantum state to be k-pairable [2]. Formally, an n-party state $|\psi\rangle$ is said to be *k-pairable* if, for every k disjoint pairs of parties $\{a_1, b_1\}, \ldots, \{a_k, b_k\}$, there exists a LOCC protocol that starts with $|\psi\rangle$ and ends up with a state where each of those k pairs of parties shares an EPR pair. Bravyi et al. studied n-party states in the case where each party holds m qubits, with m ranging from 1 to $\log(n)$. In the case where each party holds at least $m = 10$ qubits, they showed the existence of k-pairable states where k is of the order of $n/\text{polylog}(n)$, which is nearly optimal when m is constant. They also showed that if one allows a logarithmic number of qubits per party, then there exist k-pairable states with $k = n/2$. Moreover, before their work, numerous variations of this problem had surfaced in the literature, some in the context of entanglement routing [16, 26, 27], and some about problems that can be described as variants of k-pairability [5, 7–9, 12, 13, 18, 24, 25].

The notion of k-pairability that we focus on in the present paper relates to the scenario that is both the most natural and challenging [2], when each party possesses precisely one qubit, *i.e.*, $m = 1$. Protocols with multi-qubit parties, require the use of quantum operations acting on two (or more) qubits, which are significantly harder to implement in all the known technologies. For instance in quantum optics, whose 'flying' qubits are well suited for pairability protocols, one-qubit operations are easy to perform using off-the-shelf standard devices, whereas two-qubit operations, like those required by the protocols using multi-qubit parties, can only be performed probabilistically with a non-negligible probability of failure [1, 14, 21, 22]. Bravyi et al. provided some results in the setup where each party holds one single qubit, although arguably weaker than those obtained in the case where each party holds at least 10 qubits. Using Reed-Muller codes, they were able to construct a k-pairable state of size exponential in k, namely $n = 2^{3k}$, leaving the existence of a k-pairable states of size $n = poly(k)$ as an open problem. They also found a 2-pairable graph state of size 10 and proved that there exists no stabilizer state on less than 10 qubits that is 2-pairable using LOCC protocol based on Pauli measurements.

A natural generalization is to consider quantum states satisfying a stronger property: for some integer k, it is possible to induce any stabilizer state on any subset of k qubits, by means of LOCC protocols. We call these states k-stabilizer universal. Stabilizer states constitute a powerful resource for multipartite quantum protocols [17, 19, 23, 28], and can be described, up to local [1] unitaries, by the formalism of graph states: a subset of quantum states which are in one-to-one correspondence with (undirected, simple) graphs. $2k$-stabilizer universality is a stronger notion than k-pairability: any $2k$-stabilizer universal state is k-pairable, as EPR pairs are stabilizer states.

Our contributions rely on the graph state formalism and the ability to characterize properties of quantum states using tools from graph theory. In particular, we reformulate k-pairability as a property of a graph (rather than a property of a quantum state), such that the graph state corresponding to a k-pairable graph, is k-pairable. Furthermore, we relate pairability to the standard notion of vertex-minor (a complete and up-to-date survey on vertex-minors can be found in [20]). A graph H is a vertex-minor of G if one can transform G into H by means of local complementations[2] and vertex deletions. If H is a vertex-minor of G then the graph state $|H\rangle$ can be obtained from $|G\rangle$ using only local Clifford operations,

[1] As we consider one qubit per party, "local" is to be understood as "on each single qubit independently".
[2] Local complementation on a vertex u consists in complementing the subgraph induced by its neighbors.

local Pauli measurements and classical communications. Dahlberg, Helsen, and Wehner proved that the converse is also true when H has no isolated vertices [10]. In [9], they proved that it is NP-complete[3] to decide whether a graph state can be transformed into a set of EPR pairs on specific qubits using using only local Clifford operations, local Pauli measurements and classical communications. In [8], they showed that it is also NP-complete to decide whether a graph state can be transformed into another one using using only local Clifford operations, local Pauli measurements and classical communications.

The graphical counterpart of k-stabilizer universal graph states are called k-vertex-minor universal graphs, introduced by some of the authors in [6]: a graph is k-vertex minor universal if it has any graph defined on any k of its vertices as a vertex minor. If a graph is k-vertex-minor universal then the corresponding graph state is k-stabilizer universal. Stabilizer universal states (and thus k-vertex-minor universal graphs) are useful in themselves beyond the fact that they imply pairability, as they can serve as a primitive for quantum protocols using multipartite entanglement. For instance, in [6], it is shown that stabilizer universal states constitute a resource to perform a robust pairability protocol, in the sense that it allows some known parties to be malicious, while ensuring the correctness of the protocol. Furthermore, the notion of stabilizer universality is stronger than the notion of pairability. Nevertheless, while previous work [6] establishes the existence of k-stabilizer universal graph states of size $n = O(k^4 \ln(k))$ and of k-pairable graph states of size $n = O(k^3 \ln^3(k))$, there are no known graph states that are k-pairable but not $2k$-stabilizer universal.

In this work, we provide both probabilistic and explicit constructions of k-stabilizer universal graph states resulting from k-vertex-minor universal graphs. While the results are interesting in themselves from a combinatorial perspective, they allow one to explicitly define quantum communication protocols: if a k-stabilizer universal graph state is prepared, and each qubit is sent to a different party, then, with the assumption that each party can perform local quantum operations and that they can share classical information, any stabilizer state on any k qubits can be generated. Note that this includes any set of disjoint EPR pairs on less than k qubits. The local operations to perform in order to induce a given subgraph state derive directly from the proofs of our results.

The main contributions of the paper are as follows. In the first part of the paper, we prove the existence of k-vertex-minor universal graphs of order $n = \Theta(k^2)$, which is optimal as shown in [6]. We adopt a probabilistic approach, exhibiting a family of random bipartite graphs of quadratic order in k, which are k-vertex-minor universal with probability going to 1 exponentially fast in k. On the practical side, in the proof we introduce an efficient algorithm that tries to generate any induced graph of order k as a vertex-minor on any k vertices of a random bipartite graph, and the proof yields a bound on the probability of failure of the algorithm. The second part of the paper focuses on explicit constructions of k-vertex-minor universal graphs. We derive our constructions from the incidence graph of the projective plane over the finite field $\mathbb{F}_q$, where q is a prime power. It is a bipartite graph of order $n = 2(q^2 + q + 1)$, with the same number $(n/2)$ of left and right vertices, corresponding respectively to points and lines of the projective plane (equivalently, 1-dimensional and 2-dimensional linear subspaces of $\mathbb{F}_q^3$). We show it satisfies the k-vertex-minor universality property, with $k = \Theta(n^{1/4})$. Furthermore, we show that the graph on the points of the projective plane, with edges connecting points corresponding to orthogonal 1-dimensional linear subspaces of $\mathbb{F}_q^3$, is k-vertex-minor universal, again with $k = \Theta(n^{1/4})$. To the best of our knowledge, these are the first explicit constructions of k-vertex-minor universal graphs of order polynomial in k, significantly improving on the previous explicit construction of k-pairable states based on Reed-Muller codes from [2], with exponential overhead.

[3] Where the size of the input is the number of bits needed to describe the given graph state.

2 Vertex-minor and stabilizer universality

The goal of this section is to cover different notions related to k-pairability and k-vertex-minor universality properties. We first define the above properties for graphs, then we discuss their implications on the corresponding graph states.

We denote a graph as $G = (V, E)$, where V is the vertex set and E is the edge set. All graphs are assumed to be undirected and simple (without loops or multiple edges). A vertex subset $S \subseteq V$ is said to be **stable** if no two vertices in S are adjacent. Bipartite graphs are denoted as $G = (L, R, E)$, where $V = L \sqcup R$, with L and R disjoint stable sets referred to as **left and right vertex sets**, respectively. To avoid possible confusion, we may sometimes write $V(G), E(G), L(G)$, or $R(G)$. A **pairing** is a graph G such that any vertex is incident to exactly one edge. Given a vertex $v \in V$, we denote by $N_G(v)$ the **neighborhood** of v in G, consisting of vertices $v \in V$ adjacent to v.

A **local complementation** on a vertex v of a graph G consists in complementing the subgraph induced by the neighborhood of v, more precisely, it leads to a graph $G \star v$ such that $V(G \star v) = V(G)$ and $E(G \star v) = E(G) \oplus E(K_{N_G(v)})$ where K_S denotes the complete graph on the vertices in S, and $\oplus$ denotes the symmetric difference of two sets. We say that G' is a **vertex-minor** of G, if G' can be obtained from G by means of local complementations and vertex deletions. Here we consider $V(G') \subseteq V(G)$ and require G' to be obtained exactly (not up to an isomorphism of graphs), meaning that there exists a sequence of graph transformations consisting of local complementations and the deletions of the vertices of $V(G) \setminus V(G')$.

▶ **Definition 1.** *Given a graph G, a vertex subset $V' \subseteq V(G)$, and an integer $k > 0$, we say that:*

- *G is k-**vertex-minor universal** on V', if $k \leqslant |V'|$ and any graph on any k vertices in V' is a vertex-minor of G.*
- *G is k-**pairable** on V', if $k \leqslant |V'|/2$ and any pairing on any $2k$ vertices in V' is a vertex-minor of G.*

If any of the above properties is satisfied with $V' = V(G)$, we say that G is k-vertex-minor universal *or that G is* k-pairable*, respectively.*

▶ **Definition 2.** *We say that a bipartite graph $G = (L, R, E)$ is **left** (resp. **right**) k-**vertex-minor universal** or k-**pairable** if the corresponding condition from Definition 1 is satisfied for $V' = L$ (resp. $V' = R$). We say that G is **two-side** k-vertex-minor universal / k-pairable if it is both left and right k-vertex-minor universal / k-pairable.*

Graph states form a standard family of quantum states that can be represented using simple undirected graphs (Ref. [17] is an excellent introduction to graph states). Given a graph $G = (V, E)$, the corresponding **graph state** $|G\rangle$ is the $|V|$-qubit state:

$$|G\rangle = \frac{1}{\sqrt{2}^{|V|}} \sum_{x \in 2^V} (-1)^{|G[x]|} |x\rangle$$

where $|G[x]|$ is the size (number of edges) of the subgraph induced by x, and $|x\rangle$ is the corresponding base vector in the Hilbert space[4].

[4] With a slight abuse of notation we identify a subset (say $x = \{u_2, u_4\}$) of the set of qubits $V = \{u_1, \ldots, u_5\}$ with its characteristic binary word ($x = 01010$).

We shall alternatively refer to the vertex set V as qubit set. A graph state $|G\rangle$ can be prepared as follows: initialize every qubit in $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ then apply for each edge of the graph a CZ gate on the corresponding pair of qubits, where $CZ : |ab\rangle \mapsto (-1)^{ab}|ab\rangle$. The graph state $|G\rangle$ is the unique quantum state (up to a global phase) that, for every vertex $u \in V$, is a fixed point of the Pauli operator $X_u Z_{N_G(u)}$.[5] Hence, graph states form a subfamily of stabilizer states. Formally, an n-qubit **stabilizer state** [15] is a quantum state that is the simultaneous eigenvector with eigenvalue 1 of n commuting and independent Pauli operators. A useful property is that any stabilizer state is related to some graph state by the application of local Clifford unitaries, and these unitaries can be computed efficiently [11]. For instance, an EPR pair is equal to $|K_2\rangle$ up to local Clifford unitaries, where K_2 is the graph with two vertices and one edge. Thus, under LOCC protocols, generating any graph state on a given set of qubits is equivalent to generating any stabilizer state. We introduce below the notion of k-stabilizer universal states.

▶ **Definition 3.** *A quantum state $|\psi\rangle$ is k-**stabilizer universal** (resp., k-**pairable**) if any stabilizer state on any k qubits in V (resp., any k EPR pairs on any $2k$ qubits in V) can be induced by means of LOCC protocols.*

If H is a vertex-minor of a G then the graph state $|H\rangle$ can be obtained from $|G\rangle$ using only local Clifford operations, local Pauli measurements and classical communications, and the converse is true when H has no isolated vertices [10]. As a pairing on $2k$ vertices has no isolated vertices, we have the following:

▶ **Proposition 4.** *A graph G is k-pairable if and only if the corresponding graph state $|G\rangle$ is k-pairable using only local Clifford operations, local Pauli measurements, and classical communication.*

In the case of vertex-minor universality and stabilizer universality, the characterization from [10] does not apply directly, because of possible isolated vertices. For instance, K_2 is not 2-vertex-minor universal since no local complementation can turn it into an empty graph. However, $|K_2\rangle$ is 2-stabilizer universal: with *e.g.* an X-measurement on each qubit, one can map the corresponding graph state (a maximally entangled pair of qubits) to the graph state composed of a tensor product of two qubits. To be able to state a characterization, a solution is to introduce *destructive* measurements (*i.e.*, the measured qubit is removed from the system and can no longer be used).

▶ **Proposition 5.** *Given two graphs G and H such that $V(H) \subseteq V(G)$, H is a vertex-minor of G if and only if $|H\rangle$ can be obtained from $|G\rangle$ (on the qubits corresponding to $V(H)$) using only local Clifford operations, local destructive Pauli measurements, and classical communications.*

Proof. Notice that a similar statement – involving non-destructive measurements and only valid when H does not contain isolated vertices – has been proved in [10] (Theorem 2.2). We provide here a direct proof of Proposition 5 which is actually slightly simpler thanks to the use of destructive measurements. In the following proof all measurements are destructive. ($\Rightarrow$) Local complementations can be implemented by means of local Clifford unitaries, and vertex deletions by means of Z-measurements together with classical communications and Pauli corrections [11]. ($\Leftarrow$) We prove the property by induction on the number of measurements. If

[5] It consists in applying $X : |a\rangle \mapsto |1-a\rangle$ on u and $Z : |a\rangle \mapsto (-1)^a|a\rangle$ on each of its neighbors in G.

there are no measurements the property is true [11]. Otherwise, let u be the first qubit to be measured. Assume u is measured according to P and C_u is the Clifford operator applied on u before the measurement. $C_u^\dagger P C_u$ is proportional to some Pauli operator $P_0 \in \{X, Y, Z\}$:

(i) if $P_0 = Z$, then the measurement of u can be interpreted as a vertex deletion and leads to $|G \setminus u\rangle$ up to Pauli corrections. By the induction hypothesis, H is a vertex minor of $G \setminus u$, thus of G.

(ii) if $P_0 = Y$, then the measurement of u can be interpreted as a Z-measurement on $|G \star u\rangle$ (up to a Clifford operator on some other qubits), thus according to (i), H is a vertex minor of $G \star u$, so is of G.

(iii) if $P_0 = X$ and $N_G(u) \neq \emptyset$, then the measurement u can be interpreted as a Y-measurement on $|G \star v\rangle$ with $v \in N_G(u)$ (up to local Clifford operations on qubits different from u), thus according to (ii) H is a vertex minor of $G \star v$, so is of G.

(iv) if $P_0 = X$ and $N_G(u) = \emptyset$, then $|G\rangle = |G \setminus u\rangle \otimes |+\rangle_u$ so after the measurement of u the state is $|G \setminus u\rangle$, thus, by the induction hypothesis, H is a vertex minor of $G \setminus u$, so is of G. ◀

▶ **Corollary 6.** *A graph G is k-vertex-minor universal if and only if the corresponding graph state $|G\rangle$ is k-stabilizer universal using only local Clifford operations, local destructive Pauli measurements, and classical communication.*

Relations between pairability, vertex-minor universality and stabilizer universality of graph and graph states, are shown in Figure 1. To the best of our knowledge, all known examples of k-stabilizer universal (resp. k-pairable) graph states come from k-vertex-minor universal (resp. k-pairable) graphs. Furthermore, to date, it is not known whether there exist k-pairable states which are not $2k$-stabilizer universal. Throughout this paper, we will essentially focus on the existence and the explicit construction of k-vertex-minor universal graphs.

$$\begin{array}{ccc} G \text{ is } 2k\text{-vertex-minor universal} & \Longrightarrow & |G\rangle \text{ is } 2k\text{-stabilizer universal} \\ \Downarrow & & \Downarrow \\ G \text{ is } k\text{-pairable} & \Longrightarrow & |G\rangle \text{ is } k\text{-pairable} \end{array}$$

Figure 1 Implications between pairability, vertex-minor universality and stabilizer universality of graphs and graph states.

3 Existence of k-vertex-minor universal graphs of order quadratic in k

Given any k, a k-vertex-minor universal graph has at least a quadratic order in k:

▶ **Proposition 7** ([6]). *If a graph G of order n is k-vertex-minor universal then*

$$k < \sqrt{2n \log_2(3)} + 2.$$

In this section we prove that this bound is tight asymptotically, *i.e.* there exists k-vertex-minor universal graphs whose order grows quadratically with k. This greatly improves over the probabilistic construction obtained by some of us in [6], where the existence of k-vertex-minor universal graphs of order $O(k^4 \ln(k))$ was proven.

▶ **Theorem 8.** *For any constant $\alpha > 2$, there exists k_0 s.t. for any $k > k_0$, there exists a k-vertex-minor universal graph G of order at most αk^2.*

The remaining of this section is a proof of Theorem 8. First we bound the probability that some graph of order k is not a vertex-minor of a random bipartite graph G, in Lemma 10. Then we bound the probability that such a random bipartite graph is k-vertex-minor universal, in Lemma 11, by defining some algorithm that tries to generate any graph as a vertex-minor of G. Finally, we prove that there exists a k-vertex-minor universal bipartite graph of quadratic order in k. More precisely, the probability of a random bipartite graph of quadratic order being k-vertex-minor universal goes to 1 exponentially fast in k:

▶ **Proposition 9.** *Fix constants $\epsilon > 0$, $c > 2$, and $c' > \frac{1+\epsilon}{\ln(2)}$. There exists k_0 s.t. for any $k > k_0$, the random bipartite graph G (the probability of an edge existing between two vertices, one in $L(G)$ and one in $R(G)$, is $1/2$, independently of the other edges) with $|L(G)| = \lfloor c' k \ln(k) \rfloor$ and $|R(G)| = \lfloor ck^2 \rfloor$, is k-vertex-minor universal with probability at least $1 - e^{-\epsilon k \ln(k)}$.*

Proposition 9 will be proved alongside Theorem 8 in this section. Notation-wise, given a set A and an integer k, $\binom{A}{k}$ refers to $\{B \subseteq A \mid |B| = k\}$.

▶ **Lemma 10.** *Consider a random bipartite graph G with $|L(G)| \geqslant k$, $|R(G)| \geqslant 4\binom{k}{2} + 5$: the probability of an edge existing between two vertices (one in $L(G)$ and one in $R(G)$) is $1/2$, independently of the other edges. Take $k \in \mathbb{N}$ and consider a set of vertices $K \in \binom{L(G)}{k}$. The probability that there exists a graph defined on K which is not a vertex-minor of G is upper bounded by $e^{-\frac{\left(\frac{|R(G)|}{4} - \binom{k}{2} + 1\right)^2}{\left(\frac{7|R(G)|}{4} - \binom{k}{2} + 1\right)}}$.*

Proof. For some $j \in \mathbb{N} \setminus \{0\}$ and $X \in \binom{R(G)}{j}$, consider the incidence matrix M_X of size $j \times \binom{k}{2}$, whose column i represents the pairs of vertices of K that are in the neighborhood of the i^{th} vertex of X, in the sense that its entries are 1 if the pair of vertices u,v is in its neighborhood, 0 else. Note that if there exists some $X \in \binom{R(G)}{\binom{k}{2}}$ whose incidence matrix M_X is of full column-rank, then any $2^{\binom{k}{2}}$ graph defined on K is a vertex-minor of G. Indeed, column number i represents the edges (resp. non-edges) of K to be toggled by a local complementation on the i^{th} vertex of X. So now we will bound the probability of such a set X existing within $R(G)$.

For this purpose we will greedily try to construct the set $X \in \binom{R(G)}{\binom{k}{2}}$, one vertex after the other, by considering each vertex in $R(G)$ one by one, and we will lower bound the probability of the event "there exists some $X \in \binom{R(G)}{\binom{k}{2}}$ whose incidence matrix M_X is of full column-rank" by the probability of success of the algorithm. The algorithm works as follows. Arbitrarily order the vertices of $R(G)$. At each step (say that we have j vertices in X at some step), suppose the corresponding matrix of incidence (of size $j \times \binom{k}{2}$) full column-rank. We consider the next vertex $u \in R(G)$ in the list: if adding its corresponding vector to M_X increases its column-rank, then we add u to X, else we remove u from the vertices to consider. The algorithm stops (and succeeds) if M_X has $\binom{k}{2}$ columns and is full column-rank. Let us show that the probability of a vertex u increasing the column-rank of M_X (if $j < \binom{k}{2}$) is lower-bounded by $1/4$.

If M_X is of rank $j < \binom{k}{2}$, there exists a non-zero vector W (*i.e.* a set of pairs of vertices of K) which is orthogonal to all j first vectors. W can be seen as the characteristic function of the edges of some graph H on the vertices of $L(G)$. Adding a vertex u to X increases the

rank of M_X if the vector U of incidence of u in K is such that $U \cdot W = 1 \mod 2$ (because then U is not in the span of M_X). Note that, if H has exactly one edge, then there is exactly probability $\frac{1}{4}$ that $U \cdot W = 1 \mod 2$ (in this case the two ends of the unique edge of H are connected to u, which happens with probability $\frac{1}{2} \times \frac{1}{2}$). As H has at least one edge, it has at least one vertex of non-zero degree z. Let us draw randomly the neighborhood of u: first we draw among the vertices of $H \setminus \{z\}$, then we add z with probability $\frac{1}{2}$. The probability that an odd number of neighbors of z are neighbors of u is $1/2$, so drawing z changes the parity of the number of edges in H whose ends are both neighbors of u, with probability $1/2$. At the end of the day there is a probability of at least $\frac{1}{4}$ that $U \cdot W = 1 \mod 2$, so that u increases the column-rank of M_X.

Finally, the algorithm fails if we encounter more than $|R(G)| - \binom{k}{2} + 1$ vertices that did not increase the column-rank of M_X. Let us introduce a random variable T that follows the distribution $B(|R(G)|, 3/4)$. The probability that the algorithm fails is upper bounded by $\Pr(T \geqslant |R(G)| - \binom{k}{2} + 1)$. We will use the Chernoff bound: With $\mu = \mathbb{E}[T] = \frac{3|R(G)|}{4}$, for any $\delta > 0$, $\Pr(T \geqslant (1+\delta)\mu) \leqslant e^{-\frac{\delta^2}{2+\delta}\mu}$. As we need $(1+\delta)\mu = |R(G)| - \binom{k}{2} + 1$, we take $\delta = \frac{|R(G)| - \binom{k}{2} + 1 - \mu}{\mu}$. From $|R(G)| \geqslant 4\binom{k}{2} + 5$ it follows that $\delta > 0$. The Chernoff bound then gives

$$\Pr\left(T \geqslant |R(G)| - \binom{k}{2} + 1\right) \leqslant e^{-\frac{\left(\frac{|R(G)| - \binom{k}{2} + 1 - \mu}{\mu}\right)^2}{\left(\frac{|R(G)| - \binom{k}{2} + 1 + \mu}{\mu}\right)}\mu} = e^{-\frac{\left(|R(G)| - \binom{k}{2} + 1 - \mu\right)^2}{\left(|R(G)| - \binom{k}{2} + 1 + \mu\right)}} = e^{-\frac{\left(\frac{|R(G)|}{4} - \binom{k}{2} + 1\right)^2}{\left(\frac{7|R(G)|}{4} - \binom{k}{2} + 1\right)}}$$

So the probability of the existence of $X \subseteq \binom{R(G)}{k}$ whose incidence matrix M_X if of full column-rank is lower bounded by $1 - e^{-\frac{\left(\frac{|R(G)|}{4} - \binom{k}{2} + 1\right)^2}{\left(\frac{7|R(G)|}{4} - \binom{k}{2} + 1\right)}}$. ◀

▶ **Lemma 11.** *Consider a random bipartite graph G with $|L(G)| \geqslant k$, $|R(G)| \geqslant 4\binom{k}{2} + 5$: the probability of an edge existing between two vertices (one in $L(G)$ and one in $R(G)$) is $1/2$, independently of the other edges. The probability that G is k-vertex-minor universal is lower bounded by*

$$1 - \left(\frac{k}{2^{|L(G)|-k+1}} + e^{-\frac{\left(\frac{|R(G)|}{4} - \binom{k}{2} + 1\right)^2}{\left(\frac{7(|R(G)|-k)}{4} - \binom{k}{2} + 1\right)}} \right) \times \binom{|L(G)| + |R(G)|}{k}$$

The proof makes use of the union bound along with Lemma 10, and can be found in the extended version of this paper [3]. Roughly speaking, the proof introduces an algorithm that makes use of pivoting to get all k vertices of some set $K \subseteq V(G)$ on the left side of the bipartite graph, in order to use Lemma 10 properly.

▶ Remark 12. Lemma 11 has concrete applications on its own right: in particular for any integer k, it yields an integer n such that there exists a (bipartite) k-vertex-minor universal graph of order n. In general, one can infer a lower bound on the probability of generating a k-vertex-minor universal graph, for any choice of k and n, using the algorithm presented in the proof of Lemma 11. A table presenting orders for which some bipartite k-vertex-minor universal graph exists, as well as orders for with a randomly generated bipartite graph is k-vertex-minor universal with at least 99% probability, for particular values of k ranging from 3 to 100, can be found in Appendix A. Surprisingly enough, we observe that a small constant additive overheard in the order of the graph is sufficient to attain a high probability of generating a k-vertex-minor universal graph.

Now we are ready to conclude. Fix some constants $c > 2$ and $c' > \frac{1}{\ln(2)}$. Let G be a random bipartite graph G with $|L(G)| = \lfloor c'k\ln(k)\rfloor$ and $|R(G)| = \lfloor ck^2\rfloor$: the probability of an edge existing between two vertices (one in $L(G)$ and one in $R(G)$) is $1/2$, independently of the other edges.

Note $n = |V| = |L(G)| + |R(G)| = \lfloor c'k\ln(k)\rfloor + \lfloor ck^2\rfloor$. Using Lemma 11, the probability that G is k-vertex-minor universal is lower bounded by

$$1 - \left(\frac{k}{2^{|L(G)|-k+1}} + e^{-\frac{\left(\frac{|R(G)|}{4} - \binom{k}{2} + 1\right)^2}{\left(\frac{7(|R(G)|-k)}{4} - \binom{k}{2} + 1\right)}} \right) \times \binom{n}{k}$$

Let us prove that this probability is positive with our choice of parameters, for some big enough k. It is sufficient to have:

$$\textbf{(1)}\quad \frac{k}{2^{|L(G)|-k+1}}\binom{n}{k} < \frac{1}{2} \quad \text{and} \quad \textbf{(2)}\quad e^{-\frac{\left(\frac{|R(G)|}{4} - \binom{k}{2} + 1\right)^2}{\left(\frac{7(|R(G)|-k)}{4} - \binom{k}{2} + 1\right)}}\binom{n}{k} < \frac{1}{2}$$

Let us show that these equations are satisfied for any large enough k. Recall that $\binom{n}{k} \leqslant 2^{nH(k/n)}$ where $H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary entropy.

(1): It is sufficient that $\log_2(k) + nH(k/n) - |L(G)| + k - 1 < -1$.

$\log_2(k) + nH(k/n) - |L(G)| + k - 1 \sim_{k\to\infty} n\frac{k}{n}\log_2(\frac{k}{n}) - c'k\ln(k) = k(\log_2(k) - \log_2(n)) - c'k\ln(k) \sim_{k\to\infty} \frac{1}{\ln(2)}k\ln(k) - c'k\ln(k)$. The choice of c' guarantees that for any large enough k, **(1)** is satisfied.

(2): It is sufficient that $nH(k/n)\ln(2) - \frac{\left(\frac{|R(G)|}{4} - \binom{k}{2} + 1\right)^2}{\left(\frac{7(|R(G)|-k)}{4} - \binom{k}{2} + 1\right)} < -\ln(2)\cdot\frac{\left(\frac{|R(G)|}{4} - \binom{k}{2} + 1\right)^2}{\left(\frac{7(|R(G)|-k)}{4} - \binom{k}{2} + 1\right)}$ $\sim_{k\to\infty} \frac{\left(\frac{ck^2}{4} - \frac{k^2}{2}\right)^2}{\left(\frac{7ck^2}{4} - \frac{k^2}{2}\right)} = k^2\frac{(c-2)^2}{4(7c-2)}$. We saw above that $nH(k/n)\ln(2) \sim_{k\to\infty} k\ln(k)$. The choice of c guarantees that for any large enough k, **(1)** is satisfied.

This proves that, for any large enough k, G of order $\lfloor c'k\ln(k)\rfloor + \lfloor ck^2\rfloor$, is k-vertex-minor universal with non-zero probability. Taking $\alpha > c$, for any large enough k, $\lfloor c'k\ln(k)\rfloor + \lfloor ck^2\rfloor \leqslant \alpha k^2$, proving Theorem 8.

Furthermore, we just saw that side **(1)** of the equation dominates **(2)** asymptotically. Thus, the probability of G being k-vertex-minor universal is roughly lower bounded by $1 - 2^{\frac{1}{\ln(2)}k\ln(k) - c'k\ln(k)} = 1 - e^{-(\ln(2)c'-1)k\ln(k)}$ as k grows. Then, for any $\epsilon > 0$ such that $\epsilon < ln(2)c' - 1$, for any large enough k, G of order $\lfloor c'k\ln(k)\rfloor + \lfloor ck^2\rfloor$, is k-vertex-minor universal with probability at least $1 - e^{-\epsilon k\ln(k)}$, proving Proposition 9.

4 Vertex-minor universal graphs from projective planes

In this section, we provide explicit constructions of families of k-vertex-minor universal graphs, of order n proportional to k^4. Thus, the order of the constructed graphs scales as the square of the asymptotically optimal graph order from Section 3. We start in Section 4.1 with some preparatory lemmas. In Section 4.2, we introduce a family of *bipartite incidence graphs* of projective planes, and study their k-pairability and k-vertex-minor universality properties. In Section 4.3 we introduce a new family of so-called *reduced graphs* from projective planes, and investigate their k-vertex-minor universality properties.

4.1 Sufficient conditions for k-pairability and k-vertex-minor universality

Below and throughout Section 4, given a graph G, a vertex $v \in V(G)$, and a vertex subset $U \subseteq V(G)$, we shall use the **shorthand notation** $N_U(v) := N_G(v) \cap U$, that is, **the set of neighbors of v that belong to U** (in such a case, we shall always ensure that the context makes the choice of G unambiguous).

The following two lemmas give sufficient conditions for a bipartite graph G to be one-side (*i.e.*, left or right) k-pairable or k-vertex-minor universal. For simplicity, we state these conditions for the set of left vertices.

▶ **Lemma 13.** *Let G be a bipartite graph satisfying the following property:*

(P) *For any set of $2k$ vertices $K = \{u_1, v_1, u_2, v_2, \ldots, u_k, v_k\} \subseteq L(G)$, there exist:*

- **(i)** *a set of k vertices $C = \{c_1, c_2, \ldots, c_k\} \subseteq L(G)$, with $C \cap K = \emptyset$, and*
- **(ii)** *a set of $2k$ vertices $S = \{\alpha_1, \beta_1, \alpha_2, \beta_2, \ldots, \alpha_k, \beta_k\} \subseteq R(G)$, such that $N_{K \cup C}(\alpha_i) = \{u_i, c_i\}$ and $N_{K \cup C}(\beta_i) = \{v_i, c_i\}$, for all $i = 1, \ldots, k$.*

Then G is left k-pairable.

Proof. We use first local complementation on vertices α_i and β_i to create edges (u_i, c_i) and (v_i, c_i), followed by local complementation on vertices c_i to create edges (u_i, v_i), as desired. It is easily seen that no edges are created between u_i and $K \setminus \{v_i\}$, or between v_i and $K \setminus \{u_i\}$. ◀

▶ **Lemma 14.** *Let G be a bipartite graph satisfying the following property:*

(VMU) *For any set of k vertices $K = \{u_1, u_2, \ldots, u_k\} \subseteq L(G)$, there exist:*

- **(i)** *a set of $k(k-1)/2$ vertices $C = \{c_{ij} \mid 1 \leqslant i < j \leqslant k\} \subseteq L(G)$, with $C \cap K = \emptyset$, and*
- **(ii)** *a set of $k(k-1)$ vertices $S = \{\alpha_{ij}, \beta_{ij} \mid 1 \leqslant i < j \leqslant k\} \subseteq R(G)$, such that $N_{K \cup C}(\alpha_{ij}) = \{u_i, c_{ij}\}$ and $N_{K \cup C}(\beta_{ij}) = \{u_j, c_{ij}\}$, for all $1 \leqslant i < j \leqslant k$.*

Then G is left k-vertex-minor universal.

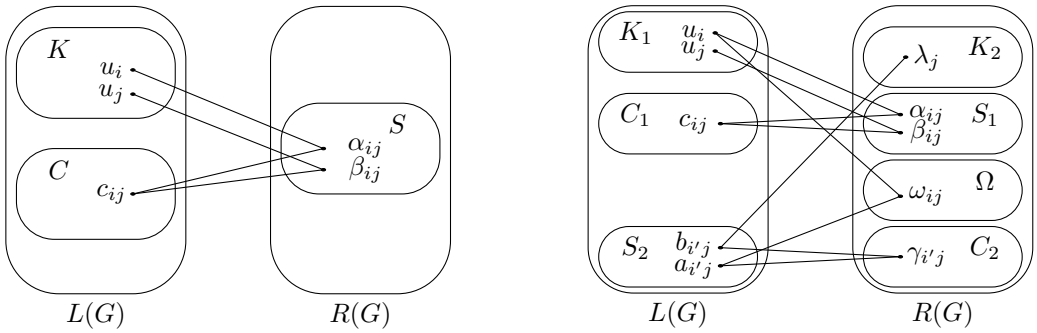
Proof. (See also Figure 2a.) The proof is similar to that of Lemma 13. To create an edge between u_i and u_j, we use first local complementation on vertices α_{ij} and β_{ij}, followed by local complementation on vertex c_{ij}. This procedure does not create any other edge between the vertices of K. ◀

Providing sufficient conditions for a bipartite graph G to be k-vertex-minor universal (on the entire vertex set) is more involved. To induce an arbitrary graph with vertex set $K = K_1 \sqcup K_2$, where $K_1 \subseteq L(G)$ and $K_2 \subseteq R(G)$, we may need to create edges with both endpoints in either K_1 or K_2, which can be dealt with by using conditions similar to those in Lemma 14, but also "toggle" (*i.e.*, either create or remove, as needed) edges between K_1 and K_2, which represents an additional difficulty. We give sufficient conditions for doing so, in the lemma below (see also Figure 2b).

▶ **Lemma 15.** *Let G be a bipartite graph satisfying the following property:*

(VMU*) *For any set of k vertices $K = K_1 \sqcup K_2$, with $K_1 = \{u_1, \ldots, u_{k_1}\} \subseteq L(G)$, and $K_2 = \{\lambda_1, \ldots, \lambda_{k_2}\} \subseteq R(G)$, there exist:*

- **(i)** *a subset $C_1 = \{c_{ij} \mid 1 \leqslant i < j \leqslant k_1\} \subseteq L(G)$, such that $C_1 \cap K_1 = \emptyset$ and $N_{K_2}(C_1) = \emptyset$,*
- **(ii)** *a subset $S_1 = \{\alpha_{ij}, \beta_{ij} \mid 1 \leqslant i < j \leqslant k_1\} \subseteq R(G)$, such that $S_1 \cap K_2 = \emptyset$ and for all $1 \leqslant i < j \leqslant k_1, N_{K_1 \sqcup C_1}(\alpha_{ij}) = \{u_i, c_{ij}\}$ and $N_{K_1 \sqcup C_1}(\beta_{ij}) = \{u_j, c_{ij}\}$,*
- **(iii)** *a subset $\Omega = \{\omega_{ij} \mid 1 \leqslant i \leqslant k_1, 1 \leqslant j \leqslant k_2\} \subseteq R(G)$ such that $\Omega \cap (K_2 \sqcup S_1) = \emptyset$ and for all $1 \leqslant i \leqslant k_1, 1 \leqslant j \leqslant k_2, N_{K_1 \sqcup C_1}(\omega_{ij}) = \{u_i\}$,*
- **(iv)** *a subset $C_2 = \{\gamma_{ij} \mid 1 \leqslant j \leqslant k_2, j < i \leqslant k_1 + k_2\} \subseteq R(G)$ such that $C_2 \cap (K_2 \sqcup S_1 \sqcup \Omega) = \emptyset$ and $N_{K_1 \sqcup C_1}(C_2) = \emptyset$,*



(a) (VMU) conditions.

(b) (VMU*) conditions where $i' := i + k_2$.

Figure 2 Illustration of the (VMU) and (VMU*) conditions from Lemma 14 and Lemma 15.

(v) *a subset* $S_2 = \{a_{ij}, b_{ij} \mid 1 \leqslant j \leqslant k_2, j < i \leqslant k_1+k_2\} \subseteq L(G)$ *such that* $S_2 \cap (K_1 \sqcup C_1) = \emptyset$ *and for all* $1 \leqslant j \leqslant k_2$, $j < i \leqslant k_1 + k_2$,
- $N_{K_2 \sqcup S_1 \sqcup \Omega \sqcup C_2}(a_{ij}) = \{\lambda_i, \gamma_{ij}\}$ *and* $N_{K_2 \sqcup S_1 \sqcup \Omega \sqcup C_2}(b_{ij}) = \{\lambda_j, \gamma_{ij}\}$, *if* $i \leqslant k_2$
- $N_{K_2 \sqcup S_1 \sqcup \Omega \sqcup C_2}(a_{ij}) = \{\omega_{(i-k_2)j}, \gamma_{ij}\}$ *and* $N_{K_2 \sqcup S_1 \sqcup \Omega \sqcup C_2}(b_{ij}) = \{\lambda_j, \gamma_{ij}\}$, *otherwise.*

Then G *is* k*-vertex-minor universal.*

Proof. We start by removing all vertices that are not in any set defined in (VMU*). Then we proceed in the following three steps.

1) In case we need to create an edge (u_i, u_j) for $1 \leqslant i < j \leqslant k_1$ between two vertices in K_1. We first use local complementations on α_{ij} and β_{ij} to create edges (u_i, c_{ij}) and (u_j, c_{ij}) (no other edges are created) and then remove α_{ij} and β_{ij}. Then, we use local complementation on c_{ij} to create the edge (u_i, u_j) (no other edges are created). Finally, we remove vertex c_{ij}, thus only the edge (u_i, u_j) has been constructed.
2) In case we need to create an edge (λ_i, λ_j) for $1 \leqslant j < i \leqslant k_2$ between two vertices in K_2. We first use local complementations on a_{ij} and b_{ij} to create edges (λ_i, γ_{ij}) and (λ_j, γ_{ij}) (no other edges are created) and then remove a_{ij} and b_{ij}. Then, we use local complementation on γ_{ij} to create the edge (λ_i, λ_j) (no other edges are created). Finally, we remove vertex γ_{ij}, thus only the edge (λ_i, λ_j) has been constructed.
3) In case we need to toggle an edge (u_i, λ_j) for $1 \leqslant i \leqslant k_1$ and $1 \leqslant j \leqslant k_2$ between two vertices in K_1 and K_2. We first use local complementations on $a_{(i+k_2)j}$ and $b_{(i+k_2)j}$ to create edges $(\omega_{ij}, \gamma_{(i+k_2)j})$ and $(\lambda_j, \gamma_{(i+k_2)j})$ (no other edges are created) and then remove $a_{(i+k_2)j}$ and $b_{(i+k_2)j}$. Then, we use local complementation on $\gamma_{(i+k_2)j}$ to create the edge (ω_{ij}, λ_j) (no other edges are created). After that, we remove vertex γ_{ij}, thus only the edge (ω_{ij}, λ_j) has been constructed. Finally, we use local complementation on ω_{ij} to create the edge (u_i, λ_j) (no other edges are created). Then, we remove vertex ω_{ij}, thus only the edge (u_i, λ_j) has been toggled. ◀

The following lemma is a generalization of Lemma 14 to the case of general (not necessarily bipartite) graphs.

▶ **Lemma 16.** *Let* G *be a graph satisfying the following property:*

(VMU$^\circ$) *For any set of* k *vertices* $K = \{u_1, u_2, \ldots, u_k\} \subseteq V(G)$*, there exist:*
- **(i)** *a set of* $k(k-1)/2$ *vertices* $C = \{c_{ij} \mid 1 \leqslant i < j \leqslant k\} \subseteq V(G)$*, such that* C *is stable,* $C \cap K = \emptyset$*, and* $N_K(c_{ij}) = \emptyset$*, for all* $1 \leqslant i < j \leqslant k$*, and*
- **(ii)** *a set of* $k(k-1)$ *vertices* $S = \{a_{ij}, b_{ij} \mid 1 \leqslant i < j \leqslant k\} \subseteq V(G)$*, such that* S *is stable,* $S \cap (K \cup C) = \emptyset$*,* $N_{K \cup C}(a_{ij}) = \{u_i, c_{ij}\}$ *and* $N_{K \cup C}(b_{ij}) = \{u_j, c_{ij}\}$*,* $\forall 1 \leqslant i < j \leqslant k$*.*

Then G *is* k*-vertex-minor universal.*

Proof. Whenever we need to create or to remove an edge between vertices $u_i, u_j \in K$, we use first local complementation on vertices a_{ij} and b_{ij} to create edges between u_i and c_{ij}, and between u_j and c_{ij}, and then we use local complementation on c_{ij}. ◀

4.2 Bipartite graphs from projective planes

Let $q > 0$ be a prime power, $\mathbb{F}_q$ be the finite field with q elements, and $\mathrm{PG}(2,q) := \left(\mathbb{F}_q^3\right)^* / \mathbb{F}_q^*$ be the *projective plane* over $\mathbb{F}_q$. *Points* and *lines* of $\mathrm{PG}(2,q)$ are identified respectively to 1-dimensional and 2-dimensional linear subspaces of $\mathbb{F}_q^3$. A line λ passes through a point a (we write $a \in \lambda$) if the 2-dimensional linear subspace of $\mathbb{F}_q^3$ corresponding to λ contains the 1-dimensional linear subspace corresponding to a. We will use the following properties of the projective plane:

- $\mathrm{PG}(2,q)$ has q^2+q+1 points and q^2+q+1 lines.
- Any line contains exactly $q+1$ points, and any point is contained in exactly $q+1$ lines.
- Any two distinct lines intersect in one point, and for any two distinct points there is one unique line containing them.

We denote by $\mathbb{G}_q$ the bipartite incidence graph of the projective plane $\mathrm{PG}(2,q)$. Precisely, the set of left vertices $L(\mathbb{G}_q)$ is the set of points of $\mathrm{PG}(2,q)$, the set of right vertices $R(\mathbb{G}_q)$ is the set of lines of $\mathrm{PG}(2,q)$, and the set of edges $E(\mathbb{G}_q)$ corresponds to incidences between points and lines, that is $E(\mathbb{G}_q) = \{(a,\lambda) \in L(\mathbb{G}_q) \times R(\mathbb{G}_q) \mid a \in \lambda\}$.

▶ **Theorem 17.** *Let k be such that $k \leqslant (q+4)/5$. Then $\mathbb{G}_q$ is two-side k-pairable.*

Proof. Due to the symmetry of $\mathbb{G}_q$, it is enough to prove it is left k-pairable. For this, we will use Lemma 13. Let $K = \{u_1, v_1, u_2, v_2, \ldots, u_k, v_k\} \subseteq L(\mathbb{G}_q)$ be a set of $2k$ points. To construct the sets $C = \{c_1, c_2, \ldots, c_k\} \subseteq L(\mathbb{G}_q)$ and $S = \{\alpha_1, \beta_1, \alpha_2, \beta_2, \ldots, \alpha_k, \beta_k\} \subseteq R(\mathbb{G}_q)$ from the property (P) in Lemma 13, we will proceed by recursion.

First, since there are $q+1$ lines passing through u_1 and $|K \setminus \{u_1\}| = 2k-1 \leqslant q$, we may choose a line α_1 passing through u_1 and not passing through any other point in $K \setminus \{u_1\}$. Similarly, let β_1 be a line passing through v_1 and not passing through any other point in $K \setminus \{v_1\}$. We take c_1 to be the intersection point between α_1 and β_1.

For $1 \leqslant j < k$, assume that we have constructed a set of j points $C_j = \{c_1, \ldots, c_j\} \subseteq L(\mathbb{G}_q)$ and a set of $2j$ lines $S_j = \{\alpha_1, \beta_1, \ldots, \alpha_j, \beta_j\} \subseteq R(\mathbb{G}_q)$, satisfying the following conditions:

(i) $C_j \cap K = \emptyset$,

(ii) $N_{K \cup C_j}(\alpha_i) = \{u_i, c_i\}$ and $N_{K \cup C_j}(\beta_i) = \{v_i, c_i\}$, for all $i = 1, \ldots, j$.

To construct $\alpha_{j+1}, \beta_{j+1}$, and c_{j+1}, we proceed in the following steps (see also Figure 3).

- **We take $\boldsymbol{\alpha_{j+1}}$ to be any line passing through $\boldsymbol{u_{j+1}}$ and not passing through any other point in $\boldsymbol{(K \setminus \{u_{j+1}\}) \cup C_j}$.**
  This is possible since $|(K \setminus \{u_{j+1}\}) \cup C_j| = 2k-1+j \leqslant 3k-2 \leqslant q$. Moreover, $\alpha_{j+1} \notin S_j$, since by construction no line in S_j passes through u_{j+1}. We further denote by $I_{j+1} \subseteq L(\mathbb{G}_q)$ the set consisting of the intersection points between α_{j+1} and the $2j$ lines in S_j. Thus, $|I_{j+1}| \leqslant 2j$.
- **We take $\boldsymbol{\beta_{j+1}}$ to be any line passing through $\boldsymbol{v_{j+1}}$ and not passing through any other point in $\boldsymbol{(K \setminus \{v_{j+1}\}) \cup C_j \cup I_{j+1}}$.**
  This is possible since $|(K \setminus \{v_{j+1}\}) \cup C_j \cup I_{j+1}| \leqslant 2k-1+3j \leqslant 5k-4 \leqslant q$. Clearly, $\beta_{j+1} \notin S_j \cup \{\alpha_{j+1}\}$, since no line in $S_j \cup \{\alpha_{j+1}\}$ passes through v_{j+1}.
- **We take $\boldsymbol{c_{j+1}}$ to be the intersection point between $\boldsymbol{\alpha_{j+1}}$ and $\boldsymbol{\beta_{j+1}}$.**
  Clearly, $c_{j+1} \notin C_j$, since neither one of α_{j+1} nor β_{j+1} passes through the points in C_j.

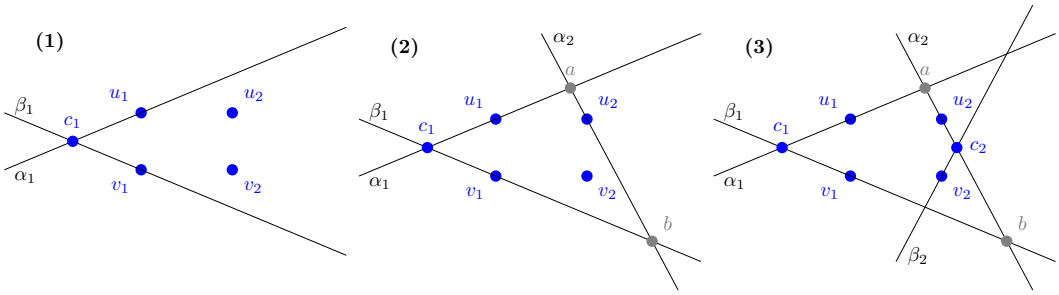


Figure 3 Recursive construction of sets C and S in the proof of of Theorem 17, for $k = 2$. (1) We chose α_1 any line passing through u_1, and not passing through v_1, u_2, v_2. Similarly, we choose β_1 passing through v_1, and not passing through u_1, u_2, v_2. We take c_1 the intersection point between α_1 and β_1. (2) We chose α_2 any line passing through u_2, and not passing through u_1, v_1, c_1, v_2. We determine the intersection points a and b of α_2 with α_1 and β_1. (3) We chose β_2 any line passing through v_2, and not passing through u_1, v_1, c_1, u_2, as well as a, b (to avoid α_2 and β_2 intersecting on these points). We take c_2 the intersection point between α_2 and β_2.

To complete our recursion, we need to prove:

(i) $C_{j+1} \cap K = \emptyset$. We only have to prove that $c_{j+1} \notin K$. This follows from the fact that each of α_{j+1} and β_{j+1} passes through only one point in K, namely u_{j+1} and v_{j+1}, respectively, and they are distinct.

(ii) $N_{K \cup C_{j+1}}(\alpha_i) = \{u_i, c_i\}$ and $N_{K \cup C_{j+1}}(\beta_i) = \{v_i, c_i\}$, for all $i = 1, \dots, j+1$.
For $i = j+1$, the above equalities follow by construction. Indeed, α_{j+1} passes through u_{j+1} and c_{j+1}, but it does not pass through any other point in $(K \setminus \{u_{j+1}\}) \cup C_j$, and similarly, β_{j+1} passes through v_{j+1} and c_{j+1}, but it does not pass through any other point in $(K \setminus \{v_{j+1}\}) \cup C_j$.
For $1 \leqslant i \leqslant j$, we only need to prove that neither α_i nor β_i passes through c_{j+1}. This follows from the fact that β_{j+1} does not pass through any point of I_{j+1}. Indeed, assuming that c_{j+1} belongs to either α_i or β_i, implies it belongs to I_{j+1}, the set of intersection points between α_{j+1} and the lines in S_j. This contradicts the fact that β_{j+1} does not pass through any point of I_{j+1}.

By recursion, we can construct sets $C := C_k$ and $S := S_k$ satisfying the property (P) from Lemma 13, and thus we conclude that $\mathbb{G}_q$ is left k-pairable. ◀

▶ **Theorem 18.** *Let k be such that $3k^2 - k - 8 \leqslant 2q$. Then $\mathbb{G}_q$ is two-side k-vertex-minor universal.*

Proof. Due to the symmetry of $\mathbb{G}_q$, it is enough to prove it is left k-vertex-minor universal. We prove $\mathbb{G}_q$ satisfies the property (VMU) from Lemma 14. Let $K = \{u_1, u_2, \dots, u_k\} \subseteq L(\mathbb{G}_q)$ be a set of k points. To construct the sets $C = \{c_{ij} \mid 1 \leqslant i < j \leqslant k\} \subseteq L(\mathbb{G}_q)$ and $S = \{\alpha_{ij}, \beta_{ij} \mid 1 \leqslant i < j \leqslant k\} \subseteq R(\mathbb{G}_q)$ from Lemma 14 we will proceed again by recursion, by running through pairs (u_i, u_j) in some particular order, say in lexicographical order with respect to indexes (i, j).

The recursion is similar to the one in the proof of Lemma 13. We construct recursively lines α_{ij} and β_{ij}, passing through u_i and u_j, respectively, and take $c_{ij} = \alpha_{ij} \cap \beta_{ij}$. In the recursion, we take α_{ij} to be any line passing through u_i and not passing through any other point in $(K \setminus \{u_i\}) \cup C_{ij}$, where $C_{ij} := \{c_{i'j'} \mid (i', j') < (i, j)\}$. Since $|(K \setminus \{u_i\}) \cup C_{ij}| \leqslant (k-1) + (k(k-1)/2 - 1) = \frac{1}{2}(k^2 + k - 4)$, such a choice of α_{ij} is possible if $k^2 + k - 4 \leqslant 2q$.

A stronger constraint on the value of k comes from the choice of β_{ij}. Indeed, for β_{ij} we take any line passing through u_j and not passing through any other point in $(K \setminus \{u_j\}) \cup C_{ij} \cup I_{ij}$, where I_{ij} is the set of intersection points between α_{ij} and the previously constructed lines $\alpha_{i'j'}$ and $\beta_{i'j'}$, with $(i', j') < (i, j)$. Since $|(K \setminus \{u_j\}) \cup C_{ij} \cup I_{ij}| \leqslant (k-1)+3(k(k-1)/2-1) = \frac{1}{2}(3k^2-k-8)$, we conclude that such a choice of β_{ij} is possible as long as $\frac{1}{2}(3k^2-k-8) \leqslant q$, as stated in the lemma. ◀

▶ **Theorem 19.** *Let k be such that $7k^2 - 16 \leqslant 4q$. Then $\mathbb{G}_q$ is k-vertex-minor universal.*

The proof is done by showing that $\mathbb{G}_q$ satisfies the property (VMU*) from Lemma 15, and can be found in the extended version of this paper [3].

4.3 Reduced graphs from projective planes

▶ **Definition 20.** *Let G be a bipartite graph and $\varphi : L(G) \to R(G)$. The φ-**reduction** of G is the graph G_φ such that:*

- *The vertex set of G_φ is the left vertex set of G, that is $V(G_\varphi) = L(G)$,*
- *There is an edge between $a, b \in V(G_\varphi)$, if $a \neq b$ and either (a and $\varphi(b)$) or (b and $\varphi(a)$) are neighbors in G, that is,*

$$E(G_\varphi) = \{(a, b) \mid a \neq b \text{ and } [\,(a, \varphi(b)) \in E(G) \text{ or } (b, \varphi(a)) \in E(G)\,]\,\}$$

*The reduction is said to be **bijective** if φ is bijective. It is said to be **symmetric** if φ is such that $(a, \varphi(b)) \in E(G) \Leftrightarrow (b, \varphi(a)) \in E(G), \forall a, b \in L(G)$.*

We enforce the condition $a \neq b$ in the definition of $E(G_\varphi)$, in order to avoid loops in case $(a, \varphi(a)) \in E(G)$ for some $a \in L(G)$.

Let G_φ be a bijective, symmetric reduction of G. For any vertex $a \in V(G_\varphi) = L(G)$, let $N_{G_\varphi}(a) \subseteq L(G)$ be the set of neighbors of a in G_φ, and $N_G(a) \subseteq R(G)$ be the set of neighbors of a in G. By definition, if $b \in N_{G_\varphi}(a)$ then $\varphi(b) \in N_G(a)$. The converse is also true, except if $\varphi(a) \in N_G(a)$, or equivalently, $(a, \varphi(a)) \in E(G)$. Hence, $N_{G_\varphi}(a) = \{b \mid \varphi(b) \in N_G(a)\} \setminus \{a\}$, and therefore:

- If $(a, \varphi(a)) \notin E(G)$, the map φ induces a bijection between $N_{G_\varphi}(a)$ and $N_G(a)$. In particular, $|N_{G_\varphi}(a)| = |N_G(a)|$.
- If $(a, \varphi(a)) \in E(G)$, the map φ induces a bijection between $N_{G_\varphi}(a)$ and $N_G \setminus \{\varphi(a)\}$. In particular, $|N_{G_\varphi}(a)| = |N_G(a)| - 1$.

In what follows, we take $\mathbb{G}_q$ to be the bipartite incidence graph of the projective plane $\mathrm{PG}(2, q)$ from the previous section. Let $\varphi : L(\mathbb{G}_q) \to R(\mathbb{G}_q)$ be defined as follows. Recall that a vertex $a \in L(\mathbb{G}_q)$ (that is, a point of the projective plane) corresponds to a 1-dimensional linear subspace of $\mathbb{F}_q^3$, while a vertex $\lambda \in R(\mathbb{G}_q)$ (that is, a line of the projective plane) corresponds to a 2-dimensional linear subspace of $\mathbb{F}_q^3$. Hence, for $a \in L(\mathbb{G}_q)$, we define $\varphi(a) \in R(\mathbb{G}_q)$ as the projective line corresponding to the 2-dimensional linear subspace orthogonal to a. Clearly, φ is bijective. It is also symmetric, since $a \in \varphi(b) \Leftrightarrow$ (a and b are orthogonal 1-dimensional linear subspaces) $\Leftrightarrow b \in \varphi(a)$. Note also that $(a, \varphi(a)) \in E(\mathbb{G}_q)$ if and only if a is self-orthogonal.

Let $\mathbb{G}_{q|\phi}$ be the bijective, symmetric reduction of $\mathbb{G}_q$ induced by φ. We will not use the explicit definition of φ, but only the fact it is bijective and symmetric. Note that $\mathbb{G}_{q|\phi}$ is a graph with $q^2 + q + 1$ vertices, and vertex degree equal to either q (vertices corresponding to self-orthogonal linear subspaces) or $q + 1$ (other vertices). The diameter of $\mathbb{G}_{q|\phi}$ is equal to 2, and for any two non-adjacent vertices $a, b \in V(\mathbb{G}_{q|\phi})$, there is a unique path of length 2 connecting them.

▶ **Theorem 21.** *Let k be such that $5k^2 - k - 10 \leqslant 2q$. Then $\mathbb{G}_{q|\phi}$ is k-vertex-minor universal.*

The proof is done by showing that $\mathbb{G}_{q|\phi}$ satisfies the property (VMU°) from Lemma 16, and can be found in the extended version of this paper [3]. Here, we briefly discuss the implications of the two constructions from Theorem 19 and Theorem 21. We denote by $\lceil x \rceil_{\mathrm{p}}$ the smallest prime power greater than or equal to a real number $x > 1$. For a given $k > 1$, let $q_2 := \left\lceil \frac{7}{4}k^2 - 4 \right\rceil_{\mathrm{p}}$ and $q_1 := \left\lceil \frac{5}{2}k^2 - \frac{1}{2}k - 5 \right\rceil_{\mathrm{p}}$ given by the inequalities in Theorem 19 (bipartite graph) and Theorem 21 (reduced graph), respectively. It follows that $\mathbb{G}_{q_2}$ is a k-vertex-minor universal of order $n_2 = 2(q_2^2 + q_2 + 1) \sim \frac{49}{8}k^4$, while $\mathbb{G}_{q_1|\phi}$ is a k-vertex-minor universal of order $n_1 = q_1^2 + q_1 + 1 \sim \frac{25}{4}k^4$ (where $\sim$ indicates asymptotic equivalence, as k goes to infinity). Thus, asymptotically, the bipartite graph construction yields k-vertex-minor universal graphs of slightly lower order than the reduced graph construction. Another interesting property of the bipartite graph is that the corresponding graph state $|\mathbb{G}_{q_2}\rangle$ is equivalent, up to local Clifford unitaries, to a Calderbank-Shor-Steane (CSS) state [4, Section IV]. However, to construct a desired graph on k-vertices of the bipartite-graph $\mathbb{G}_{q_2}$, we need to follow Lemma 15, thus to construct the sets $C_1, C_2, S_1, S_2, \Omega$ therein, which is done by following the steps highlighted in bold in the proof of Theorem 19. Note that this directly translates into a LOCC protocol to induce a desired graph state on k qubits of the state $|\mathbb{G}_{q_2}\rangle$, using Proposition 5. For the reduced graph the corresponding protocol is simpler, as we only have to construct the sets C, S from Lemma 16, which is again done by following the steps highlighted in bold in the proof of Theorem 21.

5 Conclusion

We showed the existence of k-vertex-minor universal graphs of order quadratic in k, which attain the optimum. This implies the existence of k-vertex-minor universal and thus k-pairable graph states with a quadratic number of qubits. Then, our study of the incidence graph of a finite projective plane exhibited two families of k-vertex-minor universal graphs of linear order in k^4. These two families being, to our knowledge, the first k-stabilizer universal quantum states, and so k-pairable quantum states, that can be constructed on a polynomial number of qubits in k.

This leaves open some questions for future work.

- The logical next step is the explicit, deterministic construction of an infinite family of k-vertex-minor universal graphs whose order is cubic, or even quadratic in k, asymptotically matching the order of the k-vertex-minor universal graphs which can be constructed in a probabilistic, non-deterministic way (although with arbitrarily high probability).
- Our probabilistic construction for k-vertex-minor universal graphs is asymptotically optimal. The graph states corresponding to $2k$-vertex-minor universal graphs are also k-pairable: however the only known lower bound on the size of k-pairable states (where one party holds only one qubit) is quasi-linear [2]. Does there exist k-pairable states with a quasi-linear number of qubits?
- Even though $2k$-stabilizer universality is a stronger requirement than k-pairability, it is not clear whether there exist k-pairable states which are not $2k$-stabilizer universal. A similar question can be asked for graphs: it is not clear whether there exist k-pairable graphs on more than 2 vertices which are not $2k$-vertex-minor universal.
- Bravyi et al. presented a construction of k-pairable states with an asymptotically optimal number of parties, in the case where each party holds at least 10 qubits [2]. How does k-stabilizer universality evolve when considering quantum communication networks where each party holds more than one qubit? Note that the construction of Bravyi et al. where each party holds at least 10 qubits does not translate well for k-stabilizer universality.

References

1 Sara Bartolucci, Patrick Birchall, Hector Bombin, Hugo Cable, Chris Dawson, Mercedes Gimeno-Segovia, Eric Johnston, Konrad Kieling, Naomi Nickerson, Mihir Pant, et al. Fusion-based quantum computation. *Nature Communications*, 14(1):912, 2023. doi:10.1038/s41467-023-36493-1.

2 Sergey Bravyi, Yash Sharma, Mario Szegedy, and Ronald de Wolf. Generating k EPR-pairs from an n-party resource state. *Quantum Information Processing*, 2023. arXiv:2211.06497.

3 Maxime Cautrès, Nathan Claudet, Mehdi Mhalla, Simon Perdrix, Valentin Savin, and Stéphan Thomassé. Vertex-minor universal graphs for generating entangled quantum subsystems, 2024. arXiv:2402.06260.

4 Kai Chen and Hoi-Kwong Lo. Multi-partite quantum cryptographic protocols with noisy GHZ states. *Quantum Information and Computation*, 7(8), November 2007. doi:10.26421/QIC7.8-1.

5 Matthias Christandl, Vladimir Lysikov, Vincent Steffan, Albert H Werner, and Freek Witteveen. The resource theory of tensor networks, 2023. arXiv:2307.07394.

6 Nathan Claudet, Mehdi Mhalla, and Simon Perdrix. Small k-pairable states, 2023. arXiv:2309.09956.

7 Patricia Contreras-Tejada, Carlos Palazuelos, and Julio I. de Vicente. Asymptotic survival of genuine multipartite entanglement in noisy quantum networks depends on the topology. *Physical Review Letters*, 128(22), 2022. doi:10.1103/physrevlett.128.220501.

8 Axel Dahlberg, Jonas Helsen, and Stephanie Wehner. How to transform graph states using single-qubit operations: computational complexity and algorithms. *Quantum Science and Technology*, 5(4):045016, September 2020. doi:10.1088/2058-9565/aba763.

9 Axel Dahlberg, Jonas Helsen, and Stephanie Wehner. Transforming graph states to Bell-pairs is NP-Complete. *Quantum*, 4:348, October 2020. doi:10.22331/q-2020-10-22-348.

10 Axel Dahlberg and Stephanie Wehner. Transforming graph states using single-qubit operations. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 376(2123):20170325, 2018. doi:10.1098/rsta.2017.0325.

11 Maarten Van den Nest, Jeroen Dehaene, and Bart De Moor. Graphical description of the action of local clifford transformations on graph states. *Physical Review A*, 69(2), February 2004. doi:10.1103/physreva.69.022316.

12 Gang Du, Tao Shang, and Jian-wei Liu. Quantum coordinated multi-point communication based on entanglement swapping. *Quantum Information Processing*, 16, March 2017. doi:10.1007/s11128-017-1558-2.

13 Alex Fischer and Don Towsley. Distributing graph states across quantum networks. In *IEEE International Conference on Quantum Computing and Engineering (QCE)*, pages 324–333, 2021. doi:10.1109/QCE52317.2021.00049.

14 Sobhan Ghanbari, Jie Lin, Benjamin MacLellan, Luc Robichaud, Piotr Roztocki, and Hoi-Kwong Lo. Optimization of deterministic photonic graph state generation via local operations, 2024. arXiv:2401.00635.

15 Daniel Gottesman. The heisenberg representation of quantum computers, 1998. arXiv:quant-ph/9807006.

16 Frederik Hahn, Anna Pappa, and Jens Eisert. Quantum network routing and local complementation. *npj Quantum Information*, 5(1):1–7, 2019. doi:10.1038/s41534-019-0191-6.

17 Marc Hein, Wolfgang Dür, Jens Eisert, Robert Raussendorf, Maarten Van den Nest, and Hans J. Briegel. Entanglement in graph states and its applications, 2006. arXiv:quant-ph/0602096.

18 Jessica Illiano, Michele Viscardi, Seid Koudia, Marcello Caleffi, and Angela Sara Cacciapuoti. Quantum internet: from medium access control to entanglement access control, 2022. arXiv:2205.11923.

19 Jérôme Javelle, Mehdi Mhalla, and Simon Perdrix. New protocols and lower bounds for quantum secret sharing with graph states. In *Conference on Quantum Computation, Communication, and Cryptography*, pages 1–12. Springer, 2012. arXiv:1109.1487.

20 Donggyu Kim and Sang-il Oum. Vertex-minors of graphs: A survey, October 2023. URL: https://dimag.ibs.re.kr/home/sangil/wp-content/uploads/sites/2/2023/10/2023vertexminors-survey-revised.pdf.

21 Seok-Hyung Lee and Hyunseok Jeong. Graph-theoretical optimization of fusion-based graph state generation. *Quantum*, 7:1212, December 2023. doi:10.22331/q-2023-12-20-1212.

22 Chao-Yang Lu, Xiao-Qi Zhou, Otfried Gühne, Wei-Bo Gao, Jin Zhang, Zhen-Sheng Yuan, Alexander Goebel, Tao Yang, and Jian-Wei Pan. Experimental entanglement of six photons in graph states. *Nature physics*, 3(2):91–95, 2007.

23 Damian Markham and Barry C. Sanders. Graph states for quantum secret sharing. *Physical Review A*, 78:042309, 2008. doi:10.1103/PhysRevA.78.042309.

24 Clément Meignant, Damian Markham, and Frédéric Grosshans. Distributing graph states over arbitrary quantum networks. *Physical Review A*, 100:052333, November 2019. doi:10.1103/PhysRevA.100.052333.

25 Jorge Miguel-Ramiro, Alexander Pirker, and Wolfgang Dür. Optimized quantum networks. *Quantum*, 7:919, February 2023. doi:10.22331/q-2023-02-09-919.

26 Mihir Pant, Hari Krovi, Don Towsley, Leandros Tassiulas, Liang Jiang, Prithwish Basu, Dirk Englund, and Saikat Guha. Routing entanglement in the quantum internet. *npj Quantum Information*, 5(1):1–9, 2019. doi:10.1038/s41534-019-0139-x.

27 Eddie Schoute, Laura Mancinska, Tanvirul Islam, Iordanis Kerenidis, and Stephanie Wehner. Shortcuts to quantum network routing, 2016. arXiv:1610.05238.

28 Péter Vrana and Matthias Christandl. Entanglement distillation from Greenberger–Horne–Zeilinger shares. *Communications in Mathematical Physics*, 352:621–627, 2017. arXiv:1603.03964.

A Some data on the size of the existence constraints

By Lemma 11, given some $k \in \mathbb{N} \setminus \{0\}$, there exists a k-vertex-minor universal bipartite graph G with $|L(G)| \geqslant k$, $|R(G)| \geqslant 4\binom{k}{2} + 5$ if

$$\left(\frac{k}{2^{|L(G)|-k+1}} + e^{-\frac{\left(\frac{|R(G)|}{4} - \binom{k}{2}+1\right)^2}{\left(\frac{7(|R(G)|-k)}{4} - \binom{k}{2}+1\right)}} \right) \times \binom{|L(G)| + |R(G)|}{k} < 1$$

In Table 1 we provide values for which there exists a k-vertex-minor universal bipartite graph of this order, for some particular values of k. In Table 2 we provide values for which a randomly generated bipartite graph is k-vertex-minor universal with at least 99% probability. Experimentally, adding a small, constant number of vertices to the randomly generated bipartite graph, greatly increases the probability of it to be k-vertex-minor universal.

Table 1 Parameters for which some k-vertex-minor universal bipartite graph exists.

k	3	4	5	6	7	8	9	10	11	12	13	14	15
$\|V(G)\|$	36	57	83	113	147	184	226	272	322	377	434	497	563
$\|L(G)\|$	18	24	32	40	48	55	63	72	80	90	97	107	115
$\|R(G)\|$	18	33	51	73	99	129	163	200	242	287	337	390	448

k	20	25	30	35	40	50	60	70	80	90	100
$\|V(G)\|$	955	1448	2041	2736	3531	5424	7718	10414	13512	17012	20912
$\|L(G)\|$	161	208	256	306	357	461	568	677	788	902	1016
$\|R(G)\|$	794	1240	1785	2430	3174	4963	7150	9737	12724	16110	19896

Table 2 Parameters for which a randomly generated bipartite graph is k-vertex-minor universal with at least 99% probability.

k	3	4	5	6	7	8	9	10	11	12	13	14	15
|V(G)|	47	68	93	123	156	194	235	281	331	385	443	505	571
$\|L(G)\|$	25	32	39	47	55	63	71	79	88	96	105	113	122
$\|R(G)\|$	22	36	54	76	101	131	164	202	243	289	338	392	449

k	20	25	30	35	40	50	60	70	80	90	100
|V(G)|	962	1456	2049	2743	3539	5431	7726	10422	13519	17019	20920
$\|L(G)\|$	167	215	263	313	364	468	575	684	795	908	1023
$\|R(G)\|$	795	1241	1786	2430	3175	4963	7151	9738	12724	16111	19897