UNIVERSALITY AND TOLERANCE AT THE TURN OF THE MILLENNIUM (Extended Abstract)

Noga Alon * Michael Capalbo † Yoshiharu Kohayakawa ‡
Vojtěch Rödl § Andrzej Ruciński ¶ Endre Szemerédi ‖

Abstract

For every $r \geq 2$ and $n > n_0(r)$, we construct explicitly a graph on n vertices with at most $n^{2-\Omega(1/r \log r)}$ edges that contains every graph on n vertices with maximum degree r as a subgraph. We observe that any such graph must have at least $\Omega(n^{2-2/r})$ edges, and prove that for every $\varepsilon > 0$ there is a graph with $\lceil (1+\varepsilon)n \rceil$ vertices and $\Theta(n^{2-1/r}(\log n)^{1/r})$ edges containing all graphs on n vertices with maximum degree r (in fact, almost all graphs with the above number of vertices and edges are such). We also show that a typical bipartite random graph G with n vertices in each color class and $\Theta(n^{2-1/2r}(\log n)^{1/2r})$ edges contains all bipartite graphs on n vertices in each color class with maximum degree r, and that even after deleting an α fraction of the edges of G, the resulting subgraph contains all bipartite graphs with $\lfloor n/C(\alpha) \rfloor$ vertices in each color class, and with maximum degree r. The study of these questions is motivated by problems in VLSI circuit design.

*Department of Mathematics, Raymond and Beverly Sackler Faculty of Exact Sciences, Tel Aviv University, Tel Aviv, Israel. Research supported in part by a USA-Israeli BSF grant, by the Israel Science Foundation and by the Hermann Minkowski Minerva Center for Geometry at Tel Aviv University. Email: noga@math.tau.ac.il.

†Department of Mathematical Sciences, The Johns Hopkins University, 3400 N. Charles Street, Baltimore, MD 21218. Supported by NSF grant CCR95085-45 and ARO grant DAAH04-96-1-0013. Email: capalbo@mts.jhu.edu.

‡Instituto de Matemática e Estatística, Universidade de São Paulo, Brazil. Research partially supported by FAPESP (Proc. 96/04505–2), by CNPq (Proc. 300334/93–1), and by MCT/FINEP under PRONEX project 107/97. Email: yoshi@ime.usp.br

§Department of Mathematics and Computer Science, Emory University, Atlanta. Research supported by NSF grant DMS 9704114. Email: rodl@mathcs.emory.edu

¶Faculty of Mathematics and Computer Science, Adam Mickiewicz University, Poznań, Poland. Research supported by KBN grant 2 P03A 032 16. Part of this research was done during the author's visit to Emory University. Email: rucinski@amu.edu.pl

‖Department of Computer Science, Rutgers University. Email: szemered@cs.rutgers.edu

1 Introduction

For a family $\mathcal{H}$ of graphs, a graph G is *$\mathcal{H}$-universal* if it contains every member of $\mathcal{H}$ as a subgraph. For example, the complete graph K_n is $\mathcal{H}_n$-universal for the family $\mathcal{H}_n$ of all graphs on at most n vertices. The construction of sparse universal graphs for various families arises in the study of VLSI circuit design, and received a considerable amount of attention, see, e.g., [6], [7] and their references. Since in some applications the cost of a vertex is higher than that of an edge, one is particularly interested in tight $\mathcal{H}$-universal graphs, i.e., graphs whose number of vertices equals $\max_{H\in\mathcal{H}} |V(H)|$.

Most of the previously known constructions of sparse universal graphs for various families are based on the existence of small separators in these families. Since here we deal with families of graphs that do not have small separators we need some novel techniques. These combine the notion of the strong chromatic number of a graph, introduced in [1], various properties of random graphs, an embedding technique based on matching theorems, developed in [3] and [16], a structure result on sparse regular pairs proved in [11], a sparse version of Szemerédi's regularity lemma, and a hypergraph packing result from [15].

Let $\mathcal{H}(r,n)$ denote the family of all (pairwise nonisomorphic) graphs on n vertices in which every degree is at most r. In this paper we study the minimum possible number of edges $M = M(r,n)$ in a graph on n vertices which is $\mathcal{H}(r,n)$-universal. An ultimate lower bound follows from the obvious inequality $\sum_{i\leq rn/2}\binom{M}{i} \geq |\mathcal{H}(r,n)|$ and the well known (see e.g. [10], Cor. 9.8, page 239) asymptotic formula for the number $L_{r,n}$ of all labelled r-regular graphs on n vertices, nr even:

$$L_{r,n} = (1+o(1))\sqrt{2}e^{-(r^2-1)/4}\left(\frac{r^{r/2}}{e^{r/2}r!}\right)^n n^{rn/2}.$$

Bounding $\binom{M}{rn/2} \leq \left(\frac{2eM}{rn}\right)^{rn/2}$ and $|\mathcal{H}(r,n)| \geq L_{r,n}/n!$ this yields the lower bound

$$M(r,n) = \Omega(n^{2-2/r})$$

for the number of edges of any $\mathcal{H}(r,n)$-universal graph on n vertices. If rn is odd, simply observe that an $\mathcal{H}(r,n)$-universal graph is also $\mathcal{H}(r,n-1)$-universal.

It follows from the celebrated Blow-up Lemma [13] that $M(r,n) = o(n^2)$. Here we obtain bounds of the form n^{2-a}, for some strictly positive a that depends only on r. Our first result provides an explicit construction, as stated in the following theorem. (Note that $M(1,n) = \lfloor n/2 \rfloor$.)

Theorem 1.1 *There exists an absolute positive constant c such that for every $r \geq 2$ and $n > n_0(r)$ there is an (explicitly described) $\mathcal{H}(r,n)$-universal graph G with n vertices and at most $n^{2-c/r\log r}$ edges.*

Thus, in view of the ultimate lower bound, the above construction is not too far from being best possible. If we allow G to have more than n vertices, and we do not insist on an explicit construction, we can get the following better estimate realized by "almost all" graphs. We say that a random graph possesses a property asymptotically almost surely, and write *a.a.s.*, if the probability of the event in question tends to 1 as $n \to \infty$.

Theorem 1.2 *For every $\varepsilon > 0$ there exists a positive constant $c = c(\varepsilon)$ such that for every $r \geq 2$ the random graph $G(\lceil (1+\varepsilon)n \rceil, p)$ with $p = cn^{-1/r}(\log n)^{1/r}$* a.a.s. *is $\mathcal{H}(r,n)$-universal. Consequently, for $n > n_0(r)$ there is an $\mathcal{H}(r,n)$-universal graph G with $\lceil (1+\varepsilon)n \rceil$ vertices and, say, at most $(1+\varepsilon)^2 cn^{2-1/r}(\log n)^{1/r}$ edges.*

A related Ramsey theoretic statement is considered by Kohayakawa, Rödl and Szemerédi [12].

With some more work we are able to get rid of the annoying factor of $1+\varepsilon$, but only in the bipartite case and for a slightly higher edge density. For $r \geq 2$ let $\mathcal{H}(r,n,n)$ be the family of bipartite graphs with n vertices in each vertex class and with maximum degree at most r. Let $G(n,n,p)$ be the random bipartite graph with n vertices in each color class and edge probability p.

Theorem 1.3 *There exists an absolute positive constant c such that, for every $r \geq 2$,* a.a.s. *$G(n,n,p)$ is $\mathcal{H}(r,n,n)$-universal, where $p = c(\log n/n)^{1/2r}$. Consequently, for $n > n_0(r)$ there is an $\mathcal{H}(r,n,n)$-universal, bipartite graph G with n vertices in each color class and at most $2cn^{2-1/2r}(\log n)^{1/2r}$ edges.*

It turns out that the same random graph enjoys a related property. For a real number α, where $0 < \alpha < 1$, we say that a graph G is *α-fault-tolerant* with respect to a family of graphs $\mathcal{H}$, if every subgraph of G with at least a $1-\alpha$ fraction of the edges of G is $\mathcal{H}$-universal. In general, restricting to bipartite graphs is unavoidable here, as for any graph G, there is a bipartite subgraph G' of G with at least half the edges of G.

Theorem 1.4 *For every $r \geq 2$ and $0 < \alpha < 1$ there exist constants $c > 0$ and $C > 0$ such that* a.a.s. *$G(n,n,p)$ is α-fault-tolerant with respect to $\mathcal{H}(r,h,h)$, where $h < n/C$ and $p = c(\log n/n)^{1/2r}$. Consequently, for $n > n_0(r)$ there is a bipartite graph G with n vertices in each color class and at most $2cn^{2-1/2r}(\log n)^{1/2r}$ edges, which is α-fault-tolerant with respect to $\mathcal{H}(r, \lfloor n/C \rfloor, \lfloor n/C \rfloor)$.*

The rest of this extended abstract is organized as follows. In Section 2 we sketch the proof of Theorem 1.1. Section 3 contains a brief description of the proofs of Theorems 1.2 and 1.3. Section 4 deals with Theorem 1.4. Finally, Section 5 contains some concluding remarks. Due to space limitations, some of the detailed proofs are given only in the appendix.

2 The strong chromatic number and universal graphs

The techniques in [7] can be used to construct $\mathcal{H}(r,n)$-universal graphs with $O(n^2/\log^2 n)$ edges. To obtain the better construction needed in the proof of Theorem 1.1 we combine a new technique with the main result of [1]. This construction, besides providing graphs with a rather small number of edges, is simple, and supplies an efficient algorithm for embedding any given member of $\mathcal{H}(r,n)$ in the graph constructed. The construction is in fact so simple that for $r = 3$ and any n which is a power of 16, say, $n = 16^s$, it can be described in one (short) sentence, as follows. The vertices are all vectors of length s over the alphabet $\{1, 2, \ldots, 16\}$, and two are adjacent if and only if they differ in all coordinates.

Let H be a graph with $|V(H)| = n$. If k divides n we say that H is *strongly k-colorable* if for any partition of $V(H)$ into pairwise disjoint sets V_i, each of cardinality k precisely, there is a proper k-vertex coloring of H in which each color class intersects each V_i in exactly one vertex. If k does not divide n, we say that H is strongly k-colorable if the graph obtained from H by adding to it $k\lceil n/k \rceil - n$ isolated vertices is strongly k-colorable. The *strong chromatic number* of H, denoted by $\chi_s(H)$, is the minimum k such that H is strongly k-colorable. For example, $\chi_s(C_6) = 3$. It is not difficult to check that if H is strongly k-colorable, then it is also strongly $(k+1)$-colorable.

The notion of strong chromatic number is studied in [1], where the following result is proved. (It is easy to see that if $\Delta(H) \leq 1$ then $\chi_s(H) \leq 2$.)

Theorem 2.1 ([1]) *For every $r \geq 2$:*
(i) There exists an absolute constant b such that if $\Delta(H) \leq r$ then $\chi_s(H) \leq br$.
(ii) If $\Delta(H) \leq r$ then $\chi_s(H) \leq 2^{r+1}$. ■

The constant b is very large, so that for small values of r the assertion of part (ii) is better than that of part (i). In addition, as mentioned in [1] there is a deterministic, polynomial time algorithm that gets as an input a graph H with maximum degree r and a partition of its set of vertices into pairwise disjoint subsets of cardinality $\lfloor br \rfloor$ each, and produces a proper vertex coloring of this graph in which every color class contains exactly one element of each of these subsets.

We next show how to apply the above result for the construction of universal graphs. It is easier to describe first the construction when the number of vertices is a power of the maximal strong chromatic number of the graphs with maximum degree $\leq r$. The general case if given in the appendix. For two integers k and s, let $G(k,s)$ denote the graph whose $n = k^s$ vertices are all vectors of length s over the alphabet $\{1, 2, \ldots, k\}$, where two are adjacent if and only if they differ in all coordinates. Note that $G(k,s)$ is $(k-1)^s$-regular, and hence its number of

edges is

$$\frac{1}{2}n(k-1)^s \leq n^2 \left(\frac{k-1}{k}\right)^{\log n/\log k} \leq n^{2-1/k\log k}.$$

Proposition 2.2 *For every two positive integers k and s, the graph $G(k,s)$ contains every graph H on $n = k^s$ vertices with $\chi_s(H) \leq k$.*

Proof: Split the vertex set V of H arbitrarily into disjoint subsets of size k each and find a proper coloring of H so that each color class contains precisely one vertex in each of the subsets. This coloring provides a partition of V into k disjoint sets $V_1, V_2, \ldots, V_k$, each being an independent set in H, where each set V_i is of cardinality precisely $n/k = k^{s-1}$. Next, split each set V_i arbitrarily into disjoint sets of size k each, and find another proper coloring of H so that each color class contains precisely one vertex in each of the sets. Let V_{ij} denote the set of all vertices colored i in the first coloring and colored j in the second. Note that each of the k^2 sets V_{ij} is of cardinality k^{s-2}, and if ij and $i'j'$ have a common coordinate, then there is no edge of H connecting a member of V_{ij} with a member of $V_{i'j'}$. Assume, now, that we have already partitioned the vertices of H into k^j sets V_u, indexed by the set of all vectors u in $\{1,2,\ldots,k\}^j$, where $j < s$ and for all u

$$|V_u| = k^{s-j} \text{ and there is no edge of } H \text{ between } V_u \text{ and } V_{u'} \text{ if } u,\ u' \text{ have a common coordinate.} \tag{1}$$

Now split each set V_u into disjoint subsets of cardinality k each, and find a proper coloring of H so that each color class contains exactly one vertex in each of the subsets. The new coloring splits each set V_u into k disjoint sets of equal cardinality according to the last coloring, and the new partition satisfies the condition (1) above, with j replaced by $j+1$.

When this process terminates, we obtain a partition of the set of vertices of H into k^s sets, each containing a single vertex. By mapping the only vertex in each set V_u of this partition, for $u \in \{1,2,\ldots,k\}^s$, to the vertex u of $G(k,s)$, we obtain the desired embedding. ■

Notice that by Proposition 2.2 and by Theorem 2.1(ii), the graph $G(16,s)$ contains every graph H on at most $n = 16^s$ vertices with maximum degree 3 and has no more than $n^{1.9767}$ edges. Moreover, by the fact that the proof of Theorem 2.1(ii) given in [1] provides a linear time algorithm for the corresponding algorithmic problem, the proof above supplies an $O(n\log n)$ algorithm for finding a copy of any such given H in $G(16,s)$. For larger values of r, Proposition 2.2 and Theorem 2.1(i), supply the assertion of Theorem 1.1 if n is a power of $\lfloor br \rfloor$, and supply an efficient deterministic algorithm for finding the required embeddings as well.

If the number of vertices is not necessarily a power of $\lfloor br \rfloor$ and we still want an $\mathcal{H}(r,n)$-universal graph with precisely n vertices, the construction has to be slightly modified. The details are given in the appendix.

3 Random graphs as universal graphs

In this section we sketch the proofs of Theorems 1.2 and 1.3, and also lay some ground for the more complicated proof of of Theorem 1.4. The full details are given in the appendix. The proofs are probabilistic, and apply the techniques from [3] and [16] (see also [4].) The proof of Theorem 1.4 requires in addition a sparse version of the Regularity Lemma and related structural results [11] and a new technique of graph embedding based on hypergraph packing [15].

We assume, whenever this is needed, that n is sufficiently large as a function of r, and omit all floor and ceiling signs, to simplify the presentation.

Consider the probability space of all graphs on n labelled vertices in which every pair of vertices forms an edge, randomly and independently, with probability p. We use the notation $G(n,p)$ to denote a graph chosen randomly according to this probability measure; i.e., for any graph G on n labeled vertices and with m edges, $P[G(n,p)=G] = p^m(1-p)^{\binom{n}{2}-m}$. Similarly, we define the bipartite random graph $G(n,n,p)$. Throughout we designate the bipartition of $G(n,n,p)$ by V_1 and V_2.

To show that a graph G is $\mathcal{H}$-universal, one has to find for each $H \in \mathcal{H}$ an embedding into G, i.e., a mapping $f : V(H) \to V(G)$ such that

(I) f is injective, and

(II) $f(x)f(y) \in E(G)$ if $xy \in E(H)$.

The proofs of Theorems 1.2, 1.3, and 1.4 are all based on the same scheme of constructing the embedding f, which can be outlined in a few steps, as described below. (This scheme was introduced in [3] and later used in a nonrandom context in [14] to provide an alternative proof of the Blow-up Lemma.)

We next describe the scheme. An independent set is *two-independent* if no two of its vertices have a common neighbor. Suppose we want to embed a graph $H \in \mathcal{H}(r,n)$ ($H \in \mathcal{H}(r,n,n)$) into a random (bipartite) graph G. In the bipartite case the two vertex classes of H are designated by X and Y.

1. Let $d = r^2 + 1$. Partition arbitrarily the vertex set of G into sets $W_1, W_2, \ldots, W_d$ of nearly equal size. (In the bipartite case, we only subdivide V_2, and only into $W_1, \ldots, W_{r^2}$.)

2. Apply the well known theorem of Hajnal and Szemerédi [9] to the square of H and obtain a partition of its vertex set into two-independent sets $Y_1, \ldots, Y_d$ of nearly equal size. (In the bipartite case, we only subdivide Y, and only into r^2 sets $Y_1, \ldots, Y_{r^2}$.)

3. Construct the embedding f of H into G. The embedding f will map each Y_i into W_i. We proceed in rounds; during round i we construct $f : Y_i \to W_i$, so the construction of f takes d rounds. (In the bipartite case, we first randomly map X into V_1, then simultanously construct $f : Y_i \to W_i$ for each $i = 1, \ldots, r^2$.)

The construction of the embedding f in Step 3 will heavily rely on finding saturating match-

ings in some auxiliary bipartite graphs. Step 2 is crucial in order to have probabilistic independence between edges of these auxiliary graphs. Step 1 is performed merely to conform with Step 2. We will expand on Step 3 outlined above in the proofs of Theorems 1.2, 1.3, and 1.4.

In [14] matchings are secured by maintaining the auxiliary graphs sufficiently dense, ε-regular and with high minimum degree. It is easy to see that such graphs have perfect matchings (this is a special case of Proposition B.2, below). As the density of our random graphs is $o(1)$ this approach does not work here.

In [3] the (perfect) matchings are forced by an old result of Erdős and Rényi [8] (cf. [10], Theorem 4.1, page 83). The auxiliary graphs are genuine random graphs themselves with edge probability at least p^r, and as long as p^r is bigger than $\log n/n$, there is *a.a.s.* a perfect matching.

This way it has been shown in [3] that for every fixed graph $H \in \mathcal{H}(r,n)$, if $p = cn^{-1/r}(\log n)^{1/r}$, for any $c > 3$, then $G(n,p)$ contains *a.a.s.* a copy of H (see e.g. [10], Theorem 4.13, page 94). Therefore, by a simple averaging argument, $G(n,p)$ with that p contains *a.a.s.* **almost all** such graphs H. To show that $G(n,p)$, or later $G(n,n,p)$, contains *a.a.s.* **all** of them, we have to find conditions that hold for a typical random graph, and such that for any graph G satisfying those conditions, the auxiliary graphs we define in the process of embedding contain the required matchings, and consequently G contains each H as a subgraph.

The existence of the required matchings is obtained using Hall's Theorem. See the appendix for more details.

4 Fault-tolerance of random bipartite graphs

The proof of Theorem 1.4 is based on a combination of a sparse version of the regularity lemma with a hypergraph packing result and several additional ideas. This proof is more complicated than the previous proofs in this paper and requires, besides Proposition B.3 and Lemma B.6, three additional lemmas. We describe these lemmas here and present the actual proof in the appendix. The first lemma is a special case of Lemma 20 in [11] (with α, γ, k, q replaced, resp., by $\xi/2, 1/2, r, p$). For a bipartite graph F with vertex classes U and W and for any non-empty subsets $U' \subset U$ and $W' \subset W$, we denote by $e_F(U', W')$ the number of edges between U' and W', and by

$$d_{p,F}(U', W') = \frac{e_F(U', W')}{p|U'||W'|} \tag{2}$$

the *p-density* of the pair (U', W') in F, where $0 < p \leq 1$. In particular, we set $d_F(U', W') = d_{1,F}(U', W')$. We say that the pair (U', W') is $(p;\varepsilon)$-regular in F if

$$|d_{p,F}(U', W') - d_{p,F}(U'', W'')| < \varepsilon \tag{3}$$

for all $U'' \subset U'$ and all $W'' \subset W'$ for which $|U''| \geq \varepsilon|U'|$ and $|W''| \geq \varepsilon|W'|$. A pair which is not $(p;\varepsilon)$-regular is sometimes called $(p;\varepsilon)$-irregular. If $U' = U$ and $W' = W$, we then also say that F is $(p;\varepsilon)$-regular. For a set $R \in [U]^r$ (that is, an r-element subset of U), we define its *joint degree* as

$$\deg_F(R) = \left| \bigcap_{x \in R} N_F(x) \right|, \tag{4}$$

that is, $\deg_F(R)$ is the number of stars (v, R). Finally, $G[U, W]$ stands for the subgraph of G induced by $U \cup W$.

Lemma 4.1 ([11]) *For all $r \geq 2$, $\xi > 0$, and $\eta > 0$, there is $\varepsilon > 0$ such that a.a.s. $G = G(n, n, p)$ with $p \geq n^{-3/5r}$ satisfies the following property. Suppose $U \subset V_1$, $W \subset V_2$ are sets of size at least $n^{2/3}$, and F is a $(p;\varepsilon)$-regular subgraph of $G[U, W]$ with $e_F(U, W) \geq \xi e_G(U, W)$. Then*

$$\left| \left\{ R \in [U]^r \ : \ \deg_F(R) < \frac{1}{2}(d_F(U, W))^r |W| \right\} \right| \leq \eta \binom{|U|}{r}. \tag{5}$$

■

Our next tool is the following sparse version of Szemerédi's celebrated Regularity Lemma (see e.g. [10], page 215, Lemma 8.18). For $0 < p < 1$, $b \geq 1$ and $\beta > 0$, call a graph Γ $(p; b, \beta)$-*bounded* if for every pair of disjoint subsets $U, W \subset V(\Gamma)$ with $|U|, |W| \geq \beta|V(\Gamma)|$ we have $d_{p,\Gamma}(U, W) \leq b$. Furthermore, let $\Pi = (\Pi_1, \ldots, \Pi_k)$ be a partition of $V(\Gamma)$ and suppose k divides $|V(\Gamma)|$. We say that this partition is $(p; \Gamma, \varepsilon, k)$-*regular* if $|\Pi_1| = |\Pi_2| = \ldots = |\Pi_k|$ and for all except at most $\varepsilon\binom{k}{2}$ choices of the indices $1 \leq i < j \leq k$, the pairs (Π_i, Π_j) are $(p;\varepsilon)$-regular in Γ. In the lemma below we begin with a bipartite graph and obtain a partition which subdivides the original bipartition.

Lemma 4.2 *For all $\varepsilon > 0$, $b \geq 1$ and $k_0 > 0$ there exist $\beta > 0$ and K such that the following holds. For every choice of the scaling factor p, and a $(p; b, \beta)$-bounded bipartite graph Γ on a vertex set $V = V_1 \cup V_2$, where $|V_1| = |V_2|$ is divisible by $K!$, there exists a subpartition $\Pi = (\Pi_1^1, \ldots, \Pi_k^1, \Pi_1^2, \ldots, \Pi_k^2)$ of (V_1, V_2) which is $(p; \Gamma, \varepsilon, 2k)$-regular for some $k \leq K$.* ■

We will also need a hypergraph packing result. As a preparation for it, given an r-uniform hypergraph $\mathcal{B}$ on m vertices and $\eta > 0$, let us define a recursive family of j-uniform hypergraphs $\mathcal{B}_j^\eta$, $j = r, r-1, \ldots, 1$. Set $\mathcal{B}_r^\eta = \mathcal{B}$ and, given $\mathcal{B}_j^\eta$, define $\mathcal{B}_{j-1}^\eta$ as the family of all $(j-1)$-tuples J which are contained in more than ηm j-tuples of $\mathcal{B}_j^\eta$, or in other words, for which $\deg_{\mathcal{B}_j^\eta}(J) > \eta m$.

Now we are ready to quote a special case of Theorem 2 from [15] with some minor changes in notation. The original theorem was proved only for bijections f, which is the tightest case. However, the proof can be literally repeated step by step also in a more relaxed setting when the hypergraph $\mathcal{N}$ has fewer vertices than $\mathcal{B}$. We say that a one-to-one function $f : V(\mathcal{N}) \to V(\mathcal{B})$

is *a packing* of $\mathcal{N}$ and $\mathcal{B}$, if for every $B \in \mathcal{B}$ and every $N \in \mathcal{N}$ we have $B \neq f(N)$, or shortly, $f(\mathcal{N}) \cap \mathcal{B} = \emptyset$, where $f(\mathcal{N})$ denotes the image of the hypergraph $\mathcal{N}$. We say that f'' is obtained from f' by a *switching* if for some v, w, we have $f'(v) = f''(w)$, $f'(w) = f''(v)$ and $f'(u) = f''(u)$ for all $u \neq v$, w.

Lemma 4.3 ([15]) *For all integers $r \geq 2$, and for all $\sigma > 0$, there exist $\eta > 0$ and m_0 such that the following holds. If $\mathcal{N}$ and $\mathcal{B}$ are two r-uniform hypergraphs on, resp., m_1 and m_2 vertices, $m_0 \leq m_1 \leq m_2$, satisfying $\Delta(\mathcal{N}) \leq r$ and $\mathcal{B}_1^{(\eta)} = \emptyset$, then at least half of all $(m_2)_{m_1}$ one-to-one functions $f' : V(\mathcal{N}) \to V(\mathcal{B})$ can be turned into a packing f of $\mathcal{N}$ and $\mathcal{B}$ by a sequence of at most σm_2 switchings.* ■

The derivation of Theorem 1.4 from these lemmas is given in the appendix.

5 Concluding remarks

It would be interesting to close the gap between the upper and the lower bound for the minimum possible number of edges in an $\mathcal{H}(r, n)$-universal graph on n vertices. Note that the lower bound holds even for the number of edges of any graph that contains a reasonable fraction of all r-regular graphs on n vertices (when rn is even).

As mentioned in the introduction, our proof of Theorem 1.1, together with the one in [1], supplies an efficient algorithm for finding an embedding of any given member of $\mathcal{H}(r, n)$ in the appropriate universal graph constructed here. The proof in [1] uses the Lovász Local Lemma, and the embedding algorithm thus requires an application of its algorithmic version, given in [5] (see also [2]). With a careful implementation, the running time is $n(\log n)^{O(1)}$, for any fixed r.

The application of the Hajnal-Szemerédi theorem in the proofs of Theorems 1.2–1.4 is not essential, but is convenient. Instead one could use the (algorithmic) packing lemma of Sauer and Spencer [17] (we would pack H and the union of $2r^2 + 2$ cliques of order $n/(2r^2 + 2)$, doubling the number of rounds). Thus, our proofs can be made algorithmic in the sense that if indeed a graph G satisfies the assertions of Lemma B.4, B.5 or B.6, then one can find an embedding of any member of $\mathcal{H}(r, n)$ in G in polynomial time, using some standard matching algorithms. However, the problem of checking whether a given graph G satisfies these assertions does not seem to be solvable by a polynomial time algorithm.

References

[1] N. Alon, The strong chromatic number of a graph, *Random Structures and Algorithms* 3 (1992), 1–7.

[2] N. Alon, A parallel algorithmic version of the local lemma, *Random Structures and Algorithms* 2 (1991), 367–378. Also: Proc. 32^{nd} Annual FOCS, IEEE (1991), 586–593.

[3] N. Alon and Z. Füredi, Spanning subgraphs of random graphs, *Graphs and Combinatorics* 8 (1992), 91–94.

[4] N. Alon and R. Yuster, Threshold functions for H-factors, *Combinatorics, Probability and Computing* 2 (1993), 137–144.

[5] J. Beck, An algorithmic approach to the Lovász Local Lemma, *Random Structures and Algorithms* 2 (1991), 343–365.

[6] S. N. Bhatt, F. Chung, F. T. Leighton and A. Rosenberg, Universal graphs for bounded-degree trees and planar graphs, *SIAM J. Disc. Math.* 2 (1989), 145–155.

[7] M. R. Capalbo and S. R. Kosaraju, Small universal graphs, Proc. STOC (1999), 741–749.

[8] P. Erdős and A. Renyi, On random matrices, *Publ. Math. Inst. Hung. Acad. Sci.* 8 (1964), 455–461

[9] A. Hajnal and E. Szemerédi, Proof of a conjecture of Erdős, in: *Combinatorial Theory and its Applications*, Vol. II (P. Erdős, A. Rényi and V. T. Sós eds.), Colloq. Math. Soc. J. Bolyai 4, North Holland, Amsterdam 1970, 601–623.

[10] S. Janson, T. Łuczak and A. Ruciński, *Random Graphs*, Wiley, New York, 2000.

[11] Y. Kohayakawa and V. Rödl, Regular pairs in sparse random graphs I, preliminary version available at `http://www.ime.usp.br/~yoshi/rpI.ps.gz`

[12] Y. Kohayakawa, V. Rödl and E. Szemerédi, in preparation.

[13] J. Komlós, G. Sárközy and E. Szemerédi, The Blow-up Lemma, *Combinatorica* 17 (1997) 109–123

[14] V. Rödl, A. Ruciński, Perfect matching in ε-regular graphs and the Blow-up Lemma, *Combinatorica* 19 (3) (1999) 437–452.

[15] V. Rödl, A. Ruciński and A. Taraz, Hypergraph packing and graph embedding, *Combinatorics, Probability and Computing* 8 (1999) 363–376.

[16] A. Ruciński, Matching and covering the vertices of a random graph by copies of a given graph, *Discrete Math.* 105 (1992), 185–197.

[17] N. Sauer and J. Spencer, Edge disjoint placement of graphs, *J. Combinatorial Theory Ser. B*, 25 (1978), 295–302.

A More details for Section 2

Lemma A.1 *Let H be a graph, such that the strong chromatic number of any graph obtained from it by adding an arbitrary number of isolated vertices is at most k, and let $V_1, V_2, \ldots, V_p$ be sets that partition $V(H)$, such that, writing $|V_i| = n_i$, the inequality $n_i \geq k(k+1)$ holds for all i. For each $1 \leq i \leq p$, and $1 \leq j \leq k+1$, let n_{ij} be an integer such that $\sum_{j=1}^{k+1} n_{ij} = n_i$ and $n_{ij} \leq \lceil n_i/(k+1) \rceil$ for all i, j. Then there is a partition of the vertices of H into $k+1$ pairwise disjoint sets $U_1, U_2, \ldots, U_{k+1}$, such that $|V_i \cap U_j| = n_{ij}$ for each i and j and such that each of the sets U_j,* **besides, possibly, the last one,** *U_{k+1}, is an independent set in H.*

Proof: Add to each set V_i the smallest required number of isolated vertices to obtain a set V_i' of cardinality divisible by k. Now split each of these modified sets V_i' to subsets of cardinality k each, where all the vertices of V_i' which are not in V_i lie in the same subset. Next, find a k-coloring so that each color class contains precisely one vertex of each of the subsets. Let $W_1, \ldots, W_k$ be the color classes. Observe that $|V_i \cap W_j| \geq \lfloor n_i/k \rfloor \geq \lceil n_i/(k+1) \rceil \geq n_{ij}$, for all i and j, where here we used the fact that $n_i \geq k(k+1)$ in the middle inequality. Now simply let U_j, for $1 \leq j \leq k$, be any subset of W_j containing precisely n_{ij} vertices of $V_i \cap W_j$ for all j, and let U_{k+1} contain all the remaining vertices. ■

Proof of Theorem 1.1: Given two integers n and k, with $n \geq (k+1)^2$, we next describe a graph $G_{k,n}$ on n vertices, and show that it contains every graph on n vertices whose strong chromatic number is at most k. We first present some terminology. Let K be the set of letters $\{1, 2, \ldots, k, *\}$, and for each integer q, let $K(q)$ denote the $(k+1)^q$ words of length q with letters in K. We specify the integer n_u, for each $u \in K(q)$, inductively on q; we first specify n_u for each $u \in K(1) = K$. Write $n = x_1 + x_2 + \ldots + x_k + x_*$, where $x_1, \ldots, x_k, x_*$ is a nonincreasing sequence of integers such that $x_* + 1 \geq x_i$ for all $i \in K$; let $n_u = x_u$ for each $u \in K = K(1)$. Note that this uniquely specifies n_u for $u \in K(1)$. Now for general q, let us assume that we have specified $n_{u'}$ for each $u' \in K(q-1)$; we next specify n_u for each $u \in K(q)$. Each $u \in K(q)$ can be written uniquely as $u'j$, with $u' \in K(q-1)$, and $j \in K$. Write $n_{u'} = x_{u'1} + \ldots + x_{u'k} + x_{u'*}$, where $x_{u'1}, x_{u'2}, \ldots, x_{u'k}, x_{u'*}$ is a nonincreasing sequence of integers such that $x_{u'*} + 1 \geq x_{u'i}$ for all $i \in K$; let $n_{u'i} = x_{u'i}$ for each $i \in K$. Note that this uniquely specifies n_u for each $u \in K(q)$, and that $\sum_{u \in K(q)} n_u = n$ for all q, and also that $n_u - n_v \leq 1$ for each $u, v \in K(q)$. We have specified n_u for each $u \in K(q)$ for each positive integer q. Now let s be an integer such that $(k+1)^s \leq n < (k+1)^{s+1}$. Observe that $n_u \leq (k+1)^2$ for each $u \in K(s-1)$.

We now present the construction of $G_{k,n}$. The vertex set V of $G_{k,n}$ consists of n vertices partitioned into $(k+1)^{s-1}$ sets, where each such set B_u corresponds to a $u \in K(s-1)$, and has cardinality n_u. The edge set E of $G_{k,n}$ can be described as follows. Let x be a vertex in B_u, and y a vertex in B_v, with u and v not necessarily distinct words in $K(s-1)$. Write $u = u_1 \ldots u_{s-1}$,

and $v = v_1 \dots v_{s-1}$, with each u_i and v_i in K. Put $xy \notin E$ if and only if there exists an index $i \leq s-1$ such that $u_i = v_i \neq *$.

Let us estimate the number of edges of $G_{k,n}$. There are precisely $\binom{s-1}{i} k^{s-1-i}$ blocks indexed by vectors with i stars, and each vertex in such a block is connected to the vertices in $k^{s-1-i}(k+1)^i$ blocks. Since each block contains at most $(k+1)^2$ vertices, the total number of edges does not exceed

$$\sum_{i=0}^{s-1} \binom{s-1}{i} k^{s-1-i} k^{s-1-i} (k+1)^i (k+1)^4 = (k^2+k+1)^{s-1}(k+1)^4.$$

Recalling that $n \geq (k+1)^s$, we conclude that the number of edges is at most

$$n^2(k+1)^2 \left(1 - \frac{k}{(k+1)^2}\right)^{s-1} \leq n^2 O(k^2 e^{-\frac{k \log n}{(k+1)^2 \log(k+1)}}) \leq n^{2-\Omega(1/k \log k)},$$

where the last inequality holds for all $n > n_0(k)$.

To complete the proof of Theorem 1.1 it suffices, in view of Theorem 2.1(i), to prove that $G_{k,n}$ contains any graph H on n vertices whose strong chromatic number does not exceed k. This is similar to the proof of Proposition 2.2, and can be done using Lemma A.1. ■

B Embedding via bipartite matchings

A standard way to guarantee a matching in a bipartite graph is via Hall's condition, which can be stated as follows. For two disjoint subsets of vertices S and T of a graph A, we write $e_A(S,T)$ for the number of edges with one endpoint in S and the other in T.

Proposition B.1 *Let $A = (Y, W, E)$ be a bipartite graph such that $|Y| = m_1$ and $|W| = m_2$, with $m_2 \geq m_1$. If $e_A(S,T) > 0$ for every two sets $S \subset Y$ and $T \subset W$ of sizes $|T| > m_2 - |S|$, then A has a matching saturating Y.* ■

We will use the above result in the proof of Theorem 1.2. There are several stronger conditions which imply Hall's condition. We list two of them to be used later in the proofs of Theorems 1.3 and 1.4. Their proofs are too easy to be given here.

Proposition B.2 *Let $A = (Y, W, E)$ be a bipartite graph such that $|Y| = |W| = n$, with minimum degree $\delta(A) \geq \delta$. If $e_A(S,T) > 0$ for every two sets $S \subset Y$ and $T \subset W$ of size δ, then A has a perfect matching.* ■

Proposition B.3 *Let $A = (Y, W, E)$ be a bipartite graph such that $|Y| = m_1$ and $|W| = m_2$, where $m_2 \geq m_1$. If there are integers δ and x, $1 \leq \delta < x$, such that*
(i) $\deg_A(y) \geq \delta$ *for every* $y \in Y$,

(ii) $e_A(S,T) \leq \delta|T||S|/x$ *for every two sets* $S \subset Y$ *and* $T \subset W$ *of size* $\delta \leq |T| < |S| < x$, *and*
(iii) $e_A(S,T) > 0$ *for every two sets* $S \subset Y$ *and* $T \subset W$ *of size* $|S| \geq x$ *and* $|T| > m_2 - |S|$,
then A *has a matching saturating* Y. ■

In order to verify some of these conditions we will need the following lemmas about properties of random graphs. Given a vertex v and a set R of at most r vertices, where $v \notin R$, we say that the pair (v,R) forms *a star* if v is joined to every vertex of R.

Lemma B.4 *Fix* $\varepsilon > 0$ *and set* $N = (1+\varepsilon)n$. *Let* V_0 *be a fixed subset of the vertex set* V *of the random graph* $G(N,p)$, *where* $|V_0| = N/d$, $d = r^2+1$ *and* $r \geq 2$. *If* $p = cn^{-1/r}(\log n)^{1/r}$, $c > (4d\varepsilon(r+1))^{-1/r}$, *then* a.a.s. $G(N,p)$ *satisfies the following properties:*
(a) There are at most $(1+\varepsilon)^2 cn^{2-1/r}(\log n)^{1/r}$ *edges.*
(b) For every collection $\mathcal{S}$ *of* $s \leq n/d$ *pairwise disjoint, non-empty subsets of* $V \setminus V_0$, *each of size at most* r, *and for every set* $T \subset V_0$ *of* $t = N/d - s$ *vertices, there is at least one star* (v,S), *where* $v \in T$ *and* $S \in \mathcal{S}$.

Proof: Part (a) follows by the standard estimates for binomial distributions (or simply by Chebyshev's inequality). To prove the assertion of part (b), note that the probability it fails is at most

$$\sum_{s=1}^{n/d} \binom{N}{r}^s \binom{N/d}{s} (1-p^r)^{st} \leq \sum_{s=1}^{n/d} N^{rs} N^s e^{-\varepsilon c^r (\log n) s/d} = \sum_{s=1}^{n/d} \left[\frac{N^{r+1}}{n^{\varepsilon c^r/d}} \right]^s = o(1/n^3). \blacksquare$$

The next two lemmas concern the bipartite random graph. Recall that the designated bipartition of $G(n,n,p)$ is (V_1, V_2).

Lemma B.5 *Set* $m = \lfloor n/r^2 \rfloor$ *and let* V_0 *be a fixed subset of* V_2, *where* $|V_0| = m$. *Then, for all* $c \geq 3$ *and* $r \geq 2$, a.a.s. *the random bipartite graph* $G(n,n,p)$, *where* $p = c(\log n/n)^{1/2r}$, *satisfies the following properties:*
(a) The minimum and maximum degree are within the range $np \pm \sqrt{n}$.
(b) For every r*-element subset* S_0 *of* V_1, *the number of stars* (v,S_0), *where* $v \in V_0$, *is at least* $mp^r/2$.
(c) For every collection $\mathcal{S}$ *of* $s = mp^r/2$ *pairwise disjoint,* r*-element subsets of* V_1, *and for every* s*-element subset* T *of* V_2, *there is at least one star* (v,S), *where* $v \in T$, *and* $S \in \mathcal{S}$.

Proof: Parts (a-b) follow trivially by Chernoff's bound.

To prove the assertion (c), observe that there are at most $\binom{n}{s} n^{rs} < \exp\{(r+1)s\log n\}$ choices of the set T and collection $\mathcal{S}$. Consider an auxiliary bipartite random graph $G(s,s,p^r)$ between the selected set T and the s r-tuples of $\mathcal{S}$, whose edges are the stars (v,S) of $G(n,n,p)$. The probability of there being no edges in $G(s,s,p^r)$ is smaller than $(1-p^r)^{s^2} < \exp\{-s^2p^r\} \leq \exp\{-\frac{3^{2r}}{2r^2} s\log n\}$. ■

Lemma B.6 *For all $c_1 > 0$ and $r \geq 2$,* a.a.s. *$G(n,n,p)$, where $p = c(\log n/n)^{1/2r}$ and $c = (5r/c_1)^{1/2r}$, $r \geq 2$, satisfies the following properties:*
(a) For every two sets $U \subset V_1$ and $W \subset V_2$ such that $\min(|U|,|W|) \geq n^{1/2r}\log n$ the number of edges $e(U,W)$ between them deviates from the expectation $|U||W|p$ by no more than $0.001|U||W|p$.
(b) For all integers t and s, $c_1p^rn \leq t < s \leq n$, for every selection $\mathcal{S}$ of s pairwise disjoint r-element subsets of V_1, and for every t-element subset T of V_2, the number of stars (v,S), where $v \in T$ and $S \in \mathcal{S}$, is not bigger than $2stp^r$.

Proof: Part (a) follows trivially by Chernoff's bound.

The proof of assertion (b) follows the lines of the proof of Lemma B.5(c). This time, however, we use Chernoff's bound (see, e.g., [10], Cor. 2.2, page 27), to argue that the probability of there being more than $2stp^r$ edges present in $G(s,s,p^r)$ is smaller than $\exp\{-stp^r/3\} \leq \exp\{-5rs\log n\}$. ■

Proof of Theorem 1.2

Let $p = cn^{-1/r}(\log n)^{1/r}$, where $c > (4d\varepsilon(r+1))^{-1/r}$, $d = r^2+1$ and $r \geq 2$. Let us set, as in Lemma B.4, $N = (1+\varepsilon)n$. Let V be a set of N vertices, and let $W_1,\ldots,W_d$ be subsets that partition V such that each W_i has cardinality N/d. Let G be any graph on V satisfying conditions (a) and (b) of Lemma B.4, with $V_0 = W_i$, for each $i = 1,\ldots,d$. By Lemma B.4, and by the fact that d is a constant independent of n, the random graph $G(N,p)$ *a.a.s.* satisfies these conditions, so to prove Theorem 1.2, it suffices to show that G is $\mathcal{H}(r,n)$-universal. More specifically, for each $H \in \mathcal{H}(r,n)$, we will show that there exists an $f : V(H) \to V$ that satisfies conditions (I) and (II) given at the beginning of the section.

Fix $H \in \mathcal{H}(r,n)$. By the Hajnal-Szemerédi Theorem there are sets $Y_1,\ldots,Y_d$ that partition $V(H)$ so that each Y_i is a two-independent set of H, and $|Y_i| = n/d$ for each i.

We will define f recursively on each Y_i, $i = 1,\ldots,d$. Let f be any injective embedding from Y_1 to W_1. Let us now assume that we have extended f to $Y_1 \cup \ldots \cup Y_i$, that $f(Y_1 \cup \ldots \cup Y_i) \subseteq W_1 \cup \ldots \cup W_i$, and that f is still injective. We now extend f to Y_{i+1}, ensuring that $f(Y_{i+1}) \subseteq W_{i+1}$.

We define an auxiliary, bipartite graph $A_f^{(i+1)}$ between Y_{i+1} and W_{i+1} where there is an edge between y and w if and only if $N_G(w) \subset f(N_{H[Y_1\cup\ldots\cup Y_i]}(y))$. Suppose that for each $y \in Y_{i+1}$, we are able to map $f(y) = w$ for some w such that $yw \in A_f^{(i+1)}$. Since Y_{i+1} is an independent set in H, that will guarantee that f satisfies (II). In order to guarantee (I) also, and therefore to prove Theorem 1.2, it suffices to show that the graph $A_f^{(i+1)}$ has a matching M_{i+1} that saturates Y_{i+1}. Then, for each $y \in Y_{i+1}$ let $f(y) = w$, where $yw \in M_{i+1}$.

For each $y \in Y_{i+1}$, let $S(y) = f(N_{H[Y_1\cup\ldots\cup Y_i]}(y))$, and let $\mathcal{S}_{i+1} = \{S(y) : y \in Y_{i+1}\}$. Note that each star in G of the form $(w,S(y))$, with $S(y) \in \mathcal{S}_{i+1}$, and $w \in W_{i+1}$ corresponds to

the edge $yw \in A_f^{(i+1)}$. Also note that $\mathcal{S}_{i+1}$ is a collection of disjoint sets in $W_1 \cup \ldots \cup W_i$. This is because Y_{i+1} is two-independent and f is injective. Note also that each $S \in \mathcal{S}_{i+1}$ has cardinality not greater than r, since the degree of y in H is at most r. Applying Lemma B.4(b), with $\mathcal{S} = \mathcal{S}_{i+1}$ and $V_0 = W_{i+1}$, we see that $A_f^{(i+1)}$ satisfies the hypothesis of Proposition B.1. Thus, $A_f^{(i+1)}$ has a matching saturating Y_{i+1}, and Theorem 1.2 follows. ■

Proof of Theorem 1.3

Let $p = c(\log n/n)^{1/2r}$, $c \geq 3$, $r \geq 2$. Assume for clarity of presentation that n is divisible by r^2. Let V_1 and V_2 be two disjoint sets of n vertices each, and let $W_1, \ldots, W_{r^2}$ be sets that partition V_2 such that $|W_k| = m = n/r^2$ for all $k = 1, \ldots, r^2$. Let G be a bipartite graph with the two color classes V_1 and V_2, and satisfying properties (a-c) of Lemma B.5 with $V_0 = W_i$, $i = 1, \ldots, r^2$. Observe that by property (a) G has at most $2cn^{2-1/2r}(\log n)^{1/2r}$ edges. Since a random graph $G(n, n, p)$ *a.a.s.* satisfies properties (a-c) of Lemma B.5, to prove Theorem 1.3, it suffices to prove that G is $\mathcal{H}(r, n, n)$-universal. More specifically, for each $H \in \mathcal{H}(r, n, n)$, we will show that there exists an $f : V(H) \to V_1 \cup V_2$ that satisfies (I) and (II).

Fix $H \in \mathcal{H}(r, n, n)$ and denote by X and Y its two vertex classes. It is easy to show that there exists a bipartite graph H' on the vertex set $X \cup Y$, that contains H as a spanning subgraph, has $\Delta(H') \leq r + 1$ and all vertices in Y have degree exactly r. Obviously, if H' can be embedded into G, then so can be H, and hence we may assume without loss of generality that H already has the above properties of H'. By the Hajnal-Szemerédi Theorem there is a partition $Y = Y_1 \cup \ldots \cup Y_{r^2}$, such that each Y_i is two-independent in H and $|Y_i| = |W_i|$, $i = 1, \ldots, r^2$.

We will first choose a suitable bijection $f : X \to V_1$, and then extend it to Y, by simultaneously specifying $f : Y_i \to W_i$ for all i. Given $f : X \to V_1$, define

$$A_f^{(i)} = (Y_i, W_i, E_f^{(i)}), \quad i = 1, 2, \ldots, r^2 \ ,$$

where there is an edge between y and w in $E_f^{(i)}$ if and only if $N_G(w) \supset f(N_H(y))$.

To prove Theorem 1.3, it suffices to show that for some $f : X \to V_1$ each $A_f^{(i)}$ has a perfect matching. To this end, we will use Proposition B.2. Let $\mathcal{S}_k = \{N_H(y) : y \in Y_i\}$. As in the proof of Theorem 1.2, each star of the form $(w, N_H(y))$, with $w \in W_i$ and $y \in Y_i$, corresponds to the edge yw of $A_f^{(i)}$. Therefore, by Lemma B.5(b) with $V_0 = W_i$ we immediately conclude that the degree of each $y \in A_f^{(i)}$ is at least $\delta = mp^r/2$. Also, by Lemma B.5(c) with $\mathcal{S}$ being any δ-element subcollection of $\{N_H(y) : y \in Y_i\}$, we know that $e_{A_f^{(i)}}(S, T) > 0$ for any subset $S \subseteq Y_i$ and any subset $T \subseteq W_i$ such that $|S| = |T| = \delta$. In view of Proposition B.2, to show that each $A_f^{(i)}$ has a perfect matching, and thus to prove Theorem 1.3, all we need now is the existence of an f such that

(*) for each $i = 1, \ldots, r^2$, every vertex of W_i has degree at least $\delta = mp^r/2$ in $A_f^{(i)}$.

To achieve this goal we will apply the probabilistic method, i.e., we will choose a bijection $f : X \to V_1$ uniformly at random and show that it *a.a.s.* satisfies condition (*).

Observe that f will satisfy (*) if for each $i = 1, \ldots, r^2$ and $w \in W_i$, there exist at least $mp^r/2$ vertices $y \in Y_i$ such that $f(N_H(y)) \subseteq N_G(w)$. Let Z_w be the number of vertices $y \in Y_i$ such that $f(N_H(y)) \subseteq N_G(w)$. Since G is assumed to satisfy Lemma B.5(a), we have $|N_G(w)| \geq np - \sqrt{n}$ for all $w \in W_i$.

We fix $w \in W_i$ and show that $P(Z_w \geq mp^r/2) = 1 - o(1/n)$. Consider the preimage $f^{-1}(N_G(w))$. It is drawn uniformly at random from the space of all subsets of X of order $n_w = |N_G(w)|$. Let Z'_w be the number of vertices $y \in Y_i$ such that $N_H(y) \subseteq f^{-1}(N_G(w))$. Then Z'_w has the same distribution as Z_w. We now change the space once again, and compare Z'_w to yet another random variable Z''_w which is easier to work with.

Let X_q be a random subset of X such that each $x \in X$ belongs to X_q independently with probability $q = n_w/n \geq p - n^{-1/2}$. Let $Z'' = |\{y : N_H(y) \subseteq X_q\}|$. Since the sets $N_H(y)$, $y \in Y_i$, are mutually disjoint, Z'' has the binomial distribution $\mathrm{Bi}(m, q^r)$ with expectation

$$\mu = mq^r \geq 2mp^r/3 \gg \sqrt{n}.$$

Hence, by Chernoff's inequality (see e.g. [10], Thm. 2.6, page 26), it follows that

$$P(Z'' \leq mp^2/2) \leq P(Z'' \leq 3\mu/4)) \leq \exp\{-\mu/48\} < \exp\left\{-\sqrt{n}\right\} \ .$$

However, by Pittel's inequality (see e.g. [10], formula (1.6), page 17),

$$P(Z_w \leq mp^r/2) = P(Z'_w \leq mp^r/2) \leq \sqrt{n_w} P(Z'' \leq mp^r/2) = o(1/n).$$

So, for each $w \in W_i$, $Z_w \geq mp^r/2$ with probability $o(1/n)$, and consequently *a.a.s.* each vertex in W_i has degree at least $mp^r/2$ in $A_f^{(i)}$. Thus, *a.a.s.* f satisfies (*), which in particular implies that there exists a bijection f such that the hypothesis of Proposition B.2 holds for $A_f^{(i)}$, yielding the existence of a perfect matching in $A_f^{(i)}$. This completes the proof of Theorem 1.3. ■

C The proof of Theorem 1.4

For convenience, we interchange the roles of α and $1 - \alpha$ in the definition of α-fault-tolerance. Given r and α, let $c_{\alpha,r} = \frac{1}{4r^2}\left(\frac{\alpha}{2}\right)^r$, and let $\eta < 1/2$ be the constant guaranteed by Lemma 4.3 applied with $\gamma = 1/2$ and $\sigma = \frac{1}{4}c_{\alpha,r}$, but also small enough to make the inequalites (8) and (10), below, true. Then Lemma 4.1, with $\xi = \frac{1000}{1001}(\alpha/2)$ and η^{2^r}/r^2 instead of η, yields an ε. In addition, we assume that $\varepsilon^2 < \min\{0.1\alpha, 1/2r^2\}$. With inputs ε^2 and $b = 1.001$, Lemma 4.2 outputs β and K. Set $c_1 = \frac{1}{2Kr^2}\left(\frac{\alpha}{2}\right)^r = 2c_{\alpha,r}/K$. We will prove Theorem 1.4 with $c = c(r, c_1)$ as in Lemma B.6 and $C = 2K$.

Let G be a bipartite graph with bipartition (V_1, V_2), where $|V_1| = |V_2| = n$, and satisfying properties (a) and (b) of Lemma B.6, as well as the conclusion of Lemma 4.1 with the input constants stated above.

Let Γ be an arbitrary subgraph of G with $|E(\Gamma)| \geq \alpha|E(G)|$. To prove Theorem 1.4, we must show that Γ is $\mathcal{H}(r,h,h)$-universal. By Lemma B.6(a) the graph G is $(p; 1.001, \beta)$-bounded for any constant β, and so is Γ. Thus, by Lemma 4.2 applied to Γ with $b = 1.001$, the scaling factor p and with ε^2, we obtain a $(p; \Gamma, \varepsilon^2, 2k)$-regular subpartition $\Pi = (\Pi_1^1, \ldots, \Pi_k^1, \Pi_1^2, \ldots, \Pi_k^2)$ of (V_1, V_2) for some k, $1 \leq k \leq K$. We claim that among the k^2 pairs (Π_i^1, Π_j^2) there is a pair (U, W), $U \subset V_1$, $W \subset V_2$, which is $(p; \varepsilon^2)$-regular in Γ and has the p-density $d_{p,\Gamma}(U, W) \geq \alpha/2 + \varepsilon^2$. (Note that then for all $U' \subset U$ and all $W' \subset W$ for which $|U'| \geq \varepsilon^2|U|$ and $|W'| \geq \varepsilon^2|W|$, we have $d_{p,\Gamma}(U', W') \geq \alpha/2$, or equivalently, $d_\Gamma(U', W') \geq \alpha p/2$.)

Indeed, using again Lemma B.6(a) and the fact that $\Gamma \subset G$, the number of edges in the $(p; \varepsilon^2)$-irregular pairs is at most $\varepsilon^2 \binom{2k}{2}(n/k)^2(1.001)p < 2\varepsilon^2 n^2(1.001)p$. Hence the remaining

$$\alpha(0.999)n^2p - 2\varepsilon^2 n^2(1.001)p > (\alpha/2 + \varepsilon^2)n^2p$$

edges of Γ all stretch along the $(p; \varepsilon^2)$-regular pairs, and by the Pigeon-Hole Principle at least one of these pairs, say (U, W), must contain at least $(\alpha/2 + \varepsilon^2)n^2p/k^2 \geq (\alpha/2 + \varepsilon^2)p|U||W|$ edges. We will show that already the subgraph $F = \Gamma[U, W]$ alone is $\mathcal{H}(r,h,h)$-universal.

Note that $|U| = |W| = n/k \geq n/K > 2h$. Set $l = n/k$ and without loss of generality assume that l is divisible by r^2. Split arbitrarily $W = W_1 \cup \ldots \cup W_{r^2}$ so that $|W_1| = \ldots = |W_{r^2}| = l/r^2$. Let us also set $m = l/r^2$.

Fix $H \in \mathcal{H}(r,h,h)$ and denote by X and Y its two vertex classes. We may assume without loss of generality that H is r-regular, since otherwise one could make it so by adding at most r^2 new vertices. Also, we may assume that h is divisible by r^2.

As in the proof of Theorem 1.3, by the Hajnal-Szemerédi Theorem, there is a partition $Y = Y_1 \cup \ldots \cup Y_{r^2}$, such that each Y_i is two-independent in H and $|Y_i| = h/r^2$. Note that for each $i = 1, \ldots, r^2$ and for every two distinct vertices y_1 and y_2 of Y_i their neighborhoods $N_H(y_1)$ and $N_H(y_2)$ are disjoint r-tuples in X. We will construct an injective embedding $f : V(H) \to U \cup W$ of H into F, such that, as in the proof of Theorem 1.3, $f(X) \subseteq U$, and $f(Y_i) \subseteq W_i$ for each $i = 1, \ldots, r^2$.

For any injection $f : X \to U$ define now r^2 auxiliary bipartite graphs

$$A_f^{(i)} = (Y_i, W_i, E_f^{(i)}) \ , i = 1, 2, \ldots, r^2 \ ,$$

where there is an edge between y and w in $E_f^{(i)}$ if and only if $N_F(w) \supset f(N_H(y))$. To prove Theorem 1.4, it suffices to show that there exists an $f : X \to U$ such that each $A_f^{(i)}$ contains a matching M_i that saturates Y_i. Indeed, then we will be able to extend f to Y: for each $y \in Y_i$, set $f(y) = w$, where $w \in W_i$ is such that $yw \in M_i$. To show there exists such an f, we use Proposition B.3 and Lemma 4.3.

First notice that condition (ii) of Proposition B.3 is satisfied for each $A_f^{(i)}$ with any $\delta \geq c_1 p^r n$ and $x = \delta/(2p^r)$ for arbitrary f. To see this, we use similar reasoning as in the proof of Theorem 1.3. Let $S \subset Y_i$, $\mathcal{S} = \{N_H(y) : y \in S\}$, and $T \subseteq W_i$ such that $\delta \leq |T| < |S| < x$. Since $e_{A_f^{(i)}}(S,T)$ equals the number of stars (v,S) in F, where $v \in T$ and $S \in \mathcal{S}$, and since $F \subset G$, we conclude by Lemma B.6(b) that

$$e_{A_f^{(i)}}(S,T) \leq 2|S||T|p^r = \delta|S||T|/x.$$

Our choice will be $\delta = 2c_{\alpha,r}p^r l$ and thus $x = c_{\alpha,r}l$. Note that $\delta \geq c_1 p^r n$ because $lK \geq lk = n$.

It remains to show that there exists an f such that each $A_f^{(i)}$, $i = 1, 2, \ldots, r^2$, satisfies conditions (i) and (iii) of Proposition B.3 simultaneously.

Our plan is to pick first a random f' and show, via Lemma 4.3, that with positive probability it satisfies a condition (i)$'$ which is weaker than (i), and a condition (iii)$'$ which is stronger than (iii). Then we will argue that the existence of any such f' implies the existence of an f'' for which conditions (i) and (iii) of Proposition B.3 hold.

To this end, we introduce some more notation and definitions. Let $\mathcal{N}$ be the hypergraph whose vertex-set is X and whose hyperedges are the sets $N_H(y)$, $y \in Y$. Since H is r-regular, note that $\mathcal{N}$ is both r-regular and r-uniform.

Now let us set $q = \alpha p/2$ for convenience, and for every $W' \subset W$ and $U' \subset U$, we define the hypergraph $\mathcal{B}(U', W')$. The vertex set of $\mathcal{B}(U', W')$ is U', and the edges of $\mathcal{B}(U', V')$ are the r-tuples R in $[U']^r$ with fewer than $\frac{1}{2}q^r|W'|$ common neighbors in W'. We set $\mathcal{B}(U') = \bigcup_{i=1}^{r^2} \mathcal{B}(U', W_i)$.

Suppose we can show that for some $U' \subseteq U$ there exists an injective function $f : X \to U'$ such that

$$f(\mathcal{N}) \cap \mathcal{B}(U') = \emptyset. \tag{6}$$

We claim that then each $A_f^{(i)}$, $i = 1, \ldots, r^2$, satisfies condition (i) of Proposition B.3. To see this, fix i and an arbitrary $y \in Y_i$ and note that (6) implies that $f(N_H(y)) \notin \mathcal{B}(U', W_i)$. This, in turn, implies that there must be at least $q^r m/2$ common neighbors of $f(N_H(y))$ in W_i, i.e., the degree of y in $A_f^{(i)}$ must be at least $q^r m/2$. Since $q^r m/2 \geq c_1 p^r n$, it follows that each $A_f^{(i)}$ satisfies (i) if f satisfies (6). Using Lemma 4.3, we will next show the existence of an f that satisfies (6) and (iii) simultaneously, .

We now describe the set U' for which such an f will be found. Set $\mathcal{B} = \mathcal{B}(U)$ and note that each subgraph $F[U, W_i]$ is $(p, (\varepsilon r)^2)$-regular and has at least

$$q|U||W_i| \geq \frac{1000}{1001}(\alpha/2)e_G(U, W_i)$$

edges, where the lower bound holds by Lemma B.6(a). Since $(\varepsilon r)^2 < \varepsilon$, Lemma 4.1 with $\xi = \frac{1000}{1001}(\alpha/2)$ and η replaced by η^{2^r}/r^2 implies that $|\mathcal{B}| < \eta' \binom{l}{r}$, where $\eta' = \eta^{2^r}$, for some positive $\eta < 1/2$.

Let us define a preliminary, recursive family of j-uniform hypergraphs $\mathcal{B}_j$, $j = r, r-1, \ldots, 1$. Set $\mathcal{B}_r = \mathcal{B}$ and, given $\mathcal{B}_j$, define $\mathcal{B}_{j-1}$ as the family of all $(j-1)$-tuples J which belong to more than $(\eta')^{1/2^{r-j+1}} l$ j-tuples of $\mathcal{B}_j$, or in other words, for which the (hyper)degree $\deg_{\mathcal{B}_j}(J) > (\eta')^{1/2^{r-j+1}} l$. One can easily prove by induction that $|\mathcal{B}_j| < (\eta')^{1/2^{r-j}} \binom{l}{j}$, which for $j = 1$ sets a bound of $(\eta')^{1/2^{r-1}} l = \eta^2 l$ for the number of "bad" vertices, i.e., the singletons which are the hyperedges of $\mathcal{B}_1$.

Let us remove them from U; the resulting set is U'. Let us also set $|U'| = l'$, and $\mathcal{B}' = \mathcal{B}(U')$. Note that $l' \geq (1-\eta^2)l$, where we recall that $l = |U|$, and so $|U'| \geq |X|$, since $|X| \leq l/2$. The proportion of bad and good r-sets may have changed, but still (since $\eta < 1/2$)

$$|\mathcal{B}'| < \eta' \binom{l}{r} < \eta \binom{l'}{r} \ .$$

Let us define $(\mathcal{B}')^\eta_r = \mathcal{B}'$ and, for each $j = r, \ldots, 2$,

$$(\mathcal{B}')^\eta_{j-1} = \{J \in [U']^{j-1} \ : \ \deg_{(\mathcal{B}')^\eta_j}(J) > \eta l'\} \ .$$

Then, it can be proved by induction that $(\mathcal{B}')^\eta_j \subseteq \mathcal{B}_j \cap [U']^j$, $j = r, r-1, \ldots, 1$, and in particular, $(\mathcal{B}')^\eta_1 = \emptyset$. Hence, by Lemma 4.3 with $\gamma = 1/2$ at least half of the injections $f' : X \to U'$ satisfy the following property (i)′:

(i)′ f' can be turned into an injective f'' that satisfies (6) by a sequence of at most $\sigma l'$ switchings.

The fact that the number of switchings needed is small is crucial, because we still need to show that the switchings lead to an f'' for which $A^{(i)}_{f''}$ also satisfies condition (iii) of Proposition B.3. To achieve this task it will be helpful to know that f' satisfies yet another property:

(iii)′ For all $i = 1, \ldots, r^2$, all $S \subset Y_i$, and all $T \subset W_i$, where $s = |S| \geq x$ and $|T| = m - s$, we have, with $\mathcal{N}_S = \{N_H(y) : y \in S\}$ and $D = 8\,(1 - \log c_{\alpha,r})$,

$$|f'(\mathcal{N}_S) \cap \mathcal{B}(U', T)| < \frac{Ds}{\log(1/\eta)} \ . \tag{7}$$

In Claim C.1, below, we show that a random injection f' *a.a.s.* satisfies property (iii)′. Taking this claim for granted, it follows that for a positive fraction of injections $f' : X \to U'$ conditions (i)′ and (iii)′ hold simultaneously. We will now show that for any such f' a series of at most $\sigma l'$ switchings leads to an injection f'' which satisfies both conditions (i) and (iii) of Proposition B.3.

Let $S \subset Y_i$ and $T \subset W_i$, where $s = |S| \geq x$ and $|T| = m - s$ For any injection $f : X \to U'$, let us call a vertex $y \in S$ *T-good under f* if $f(N_H(y)) \notin \mathcal{B}(U', T)$. By definition, every T-good

vertex sends in $A_f^{(i)}$ at least $\frac{1}{2}q^r|T|$ edges to T. Property (iii)$'$ asserts that under f' there are at least $s - \frac{Ds}{\log(1/\eta)}$ T-good vertices in S.

When transforming f' to f'' by a series of at most

$$\sigma l' \le \sigma l = \frac{1}{4} c_{\alpha,r} l = \frac{x}{4} \le \frac{s}{4}$$

switchings, at most twice that many r-tuples of each $f'(\mathcal{N}_i)$ will be moved. Hence, for any T and S, at least

$$s - \frac{Ds}{\log(1/\eta)} - 2\sigma l' \ge \frac{s}{2} - \frac{Ds}{\log(1/\eta)} > 0 \tag{8}$$

vertices of S will be still T-good under f'', yielding condition (iii) of Proposition B.3 with a surplus. At the same time, by the definition of f'', it satisfies property (6), and consequently condition (i) of Proposition B.3 as well.

It remains to formulate and prove Claim C.1.

Claim C.1 *A random injective $f' : X \to U'$* a.a.s. *satisfies (iii)$'$.*

Proof: The number of choices of i, S and T is at most

$$r^2 \binom{h/r^2}{s} \binom{m}{s} < r^2 \binom{l}{s}^2 .$$

Since $|U'| \ge (1-\eta^2)l$ and $|T| \ge (l-h)/r^2 \ge l/2r^2$, the pair (U', T) is $(p; 2\varepsilon^2 r^2)$-regular in F and has at least $q|U'||T| \ge \frac{1000}{1001}(\alpha/2)e_G(U', T)$ edges, where the lower bound holds, again, by Lemma B.6(a). Since $2\varepsilon^2 r^2 < \varepsilon$, another application of Lemma 4.1 (with the same parameters as before), yields that

$$|\mathcal{B}(U', T)| < \eta' \binom{l'}{r} \le \eta \binom{l'}{r} .$$

We may think of a random f' as of a sequence of random selections of images of the elements of X. As the order in which the images are assigned is immaterial, we may as well begin with the r-tuples belonging to $\mathcal{N}_S$. Then, the probability that the j-th of them will be mapped into an r-tuple of $\mathcal{B}(U', T)$ is at most $\eta\binom{l'}{r} / \binom{l'-(j-1)r}{r}$. Note that $r|\mathcal{N}_S| \le h/r < l'/2$ with room to spare. Thus, the probability of the event opposite to (iii)$'$ can be bounded by

$$r^2 \binom{l}{s}^2 P\left(Z \ge \frac{Ds}{\log(1/\eta)} \right), \tag{9}$$

where Z is a random variable with the binomial distribution $\mathrm{Bi}(s, \rho)$ with parameter

$$\rho = \frac{\eta\binom{l'}{r}}{\binom{l'/2}{r}} < 3^r \eta .$$

To estimate the tail probability, we employ the trivial bound

$$P(Z \geq z) < \binom{s}{z} \rho^z < (es\rho/z)^z$$

with $z = \frac{Ds}{\log(1/\eta)}$. Since

$$\frac{1 + r\log 3 - \log D + \log\log(1/\eta) - \log(1/\eta)}{\log(1/\eta)} < -1/2 \ , \tag{10}$$

we finally get

$$r^2 \binom{l}{s}^2 P\left(Z \geq \frac{Ds}{\log(1/\eta)}\right) < r^2 \left((el/s)^2 e^{-D/2}\right)^s = r^2 e^{-Ds/4} = o(1) \ . \tag{11}$$

This completes the proof. ■