Constructing Ramsey graphs from small probability spaces

Moni Naor
IBM Almaden Research Center
650 Harry Road
San-Jose CA 95120
naor@almaden.ibm.com

Abstract

The problem of explicitly constructing Ramsey graphs, i.e graphs that do not have a large clique or independent set is considered. We provide an elementary construction of a graph with the property that there is no clique or independent set of t of nodes, while the graph size is $t^{\frac{\sqrt{\log\log t}}{\log\log\log t}}$. The construction is based on taking the product of all graphs in a distribution that is known to have mostly Ramsey graphs.

Keywords: Ramsey Graphs, Graph Products, Probabilistic Method, Derandomization.

1 Introduction

Ramsey Theory asserts that every graph on N nodes must contain a clique or independent set of size $\frac{1}{2}\log N$. On the other hand, Erdös [5] has shown that there are graphs on N nodes that do not contain (as a subgraph) a clique or independent set on $2\log N$ vertices and in fact most graphs on N nodes have this property. His proof, which is the precursor of the "Probabilistic Method", did not establish a way of constructing such graphs. It is still an open problem to construct graphs that achieve these bounds. (See [8] for information about Ramsey Theory and [3] for a thorough discussion of the probabilistic method.)

For a given size t, one might ask what is the largest (as a function of t) graph that can be explicitly constructed which does not contain a clique or independent set of size t. Erdös posed as a challenge the problem of constructing a graph whose size is superpolynomial in t and does not contain a clique or independent set of size t. The challenge was answered by Frankl [6] and Frankl and Wilson [7] who showed an explicit way of constructing graphs that are of size $t^{\frac{\log t}{\log\log t}}$.

The goal of this paper is to present an elementary construction of a graph whose size is superpolynomial in t (the size we know that there is no subgraph which is a clique or independent set). Our construction is not as good as [7], the graph size is $t^{\frac{c\sqrt{\log\log t}}{\log\log\log t}}$ for some constant c.

A well known conjecture in this area is that the Paley graph is a Ramsey graph. The Paley graph is defined for every prime p which is congruent to 1 mod 4. There is an edge between nodes i and j iff $i-j$ is a quadratic residue mod p. An interesting consequence of our construction is that a closely related graph can be shown to be a (weak) Ramsey graph.

Our construction of Ramsey graphs is based on combining many graphs, most of which are known to be good, without testing which are the bad ones. The fact that most of graphs are good compensates for the bad ones.

Remark: Our construction is inspired by Justesen's construction of good error correcting codes [9] (see [10] for more information on codes). It was known that good binary codes can be obtained by concatenating a good code over a large alphabet (which can be explicitly constructed) with good codes that map the large alphabet to the small one. The existence of this code was only proved non-constructively. Justesen suggested using a collection of codes, most of which were known to be good, instead of one good code.

2 The construction

Our starting point is Abbot's observation [1] about products of graphs: let G_1 and G_2 be graphs on n_1 and n_2 nodes respectively that do not contain a clique or independent set of size k_1 and k_2 respectively, then their product is a graph on $n_1 \cdot n_2$ nodes that does not contain a k_1k_2 clique or independent set. The product here means that (u_1, u_2) is connected to (v_1, v_2) if u_1 is different from v_1 and they are connected in G_1 or if $u_1 = v_1$ and u_2 is connected to v_2 in G_2. Babai and Frankl (see [4] pp. 46) suggested this as a method that starts from a small graph with a certain relationship between the size of the graph and the size of a minimum non monochromatic subgraph and generates a large graph with the same relationship. Thus, it can be used as an "existential argument for an explicit construction" of graphs whose size is polynomial in the non monochromatic subgraph, for any fixed polynomial.

We will use it slightly differently, by taking the products of all the graphs of a certain distribution, where the probability of a graph being "good" is high. Note that if we have a collection of graphs $G_1, G_2, \ldots G_m$ of size $n_1, n_2, \ldots n_m$ and number $k_1, k_2, \ldots k_m$ such that G_i does not contain a clique or independent set of size k_i, then the graph H which is the product of $G_1, G_2, \ldots G_m$ is of size $\prod_{i=1}^m n_i$ and does not contain a clique or independent set of size $\prod_{i=1}^m k_i$.

Let $\mathcal{D}$ be a collection of m graphs on n nodes such that the probability that a graph G drawn from $\mathcal{D}$ has either a clique or an independent set of size k is at most α. For at most αm of the graphs which have a clique or independent set of size larger than k we assume nothing, i.e. they might have a clique or independent of size n. By the discussion above we have

Lemma 1 *Consider the graph H obtained by taking the product of all the graphs in the collection $\mathcal{D}$. Then the number of nodes in H is $N = n^m$ and there is no clique or independent set of size*

$t = k^{(1-\alpha)m} n^{\alpha m}$. *If* $\alpha < \frac{1}{\log n}$, *then* $t < (2k)^m$.

In order to apply the lemma, what we should do is try to come up for k and n (where k is much smaller than n ($\approx \log n$)) with as small a collection $\mathcal{D}$ as possible that has the desired property with $\alpha \approx \frac{1}{\log n}$.

Example: Take $\mathcal{D}$ to be the set of all graph on n nodes and k to be $2 \log n$. We know that for this collection $\alpha < \frac{1}{\log n}$. Therefore the graph H in Lemma 1 is on $N = n^{2^{\binom{n}{2}}}$ nodes and does not contain a clique or independent set on $t = (2 \log n)^{2^{\binom{n}{2}}}$ nodes, i.e. $N \geq t^{\frac{\log\log\log t}{\log\log\log\log t}}$. As we shall see in the next section, by taking smaller sample spaces we can do better.

3 A construction based on small bias probability spaces

We now introduce small bias probability spaces, as defined in [11]. A probability space with n random variables in $\{0,1\}$ is called `k-wise ε-bias` if for any k or fewer random variables the probabilities that their parity is 0 or 1 is differ by at most ϵ. It is known that in a k-wise ϵ-bias probability space, the probability that any k given random variables are all '0' or all '1' is at most $(2^{-k+1} + 2^{k/2}\epsilon)$, since the variation distance of the distribution of any k random variables from the uniform distribution is at most $2^{k/2}\epsilon$.

Thus, if the edges of a graph are chosen from a $\binom{k}{2}$-wise ϵ bias probability space on $\binom{n}{2}$ random variables, then the probability that there is a clique or independent set of size k is at most $\binom{n}{k} \cdot (2^{-\binom{k}{2}+1} + 2^{\binom{k}{2}/2}\epsilon)$. Taking k to be $2 \log n$ and ϵ to be 2^{-k^2} we get that this probability is less than $\frac{1}{\log n}$.

Consider now a $\mathcal{D}$ that is defined by this probability space, i.e. every graph corresponds to a point in the probability space. The constructions of ϵ-bias probability spaces in [11] and [2] are of size $(n/\epsilon)^c$ for some fixed c. Therefore, $m = 2^{c'k^2}$ for some fixed c'. For the graph H in Lemma 1 we have that $N = 2^{k 2^{c'k^2}}$ and t is $2^{2^{c'k^2}}$, i.e. $N \geq t^{\frac{c'\sqrt{\log\log t}}{\log\log\log t}}$.

We now take a concrete example of an k-wise ϵ-bias probability space given in [2]. It is based on quadratic characters. Let p be a prime which is $1 \bmod 4$ such that $p \geq (k/\epsilon)^2$ (and also greater than $\binom{n}{2}$). A point in the probability space is defined by $i \in Z_p$. The random variable x_j at point i is the quadratic character of $i + j \bmod p$, i.e if $i + j$ is a quadratic residue modulo p, then x_j is 1 and it is 0 otherwise. Since the random variables we are interested in are edges, for nodes a and b such that $1 \leq b < a \leq n$ we associate $x_{a(a-1)/2+b}$ with the edge (a, b).

The description of the graph $H_n = (V, E)$ is now: fix $k = 2 \log n$ and $p > k^2 2^{k^2}$.

$$V = \{(a_1, a_2, \ldots a_{p-1}) | 1 \leq a_i \leq n\}$$

To determine whether there is an edge between two nodes $a = (a_1, a_2, \ldots a_{p-1})$ and $b = (b_1, b_2, \ldots b_{p-1})$ let be i the first index where $a_i \neq b_i$ (i.e. $a_1, a_2, \ldots a_{i-1} = b_1, b_2, \ldots b_{i-1}$). In case $b_i < a_i$, then the quadratic residuosity modulo p of $i + a_i(a_i - 1)/2 + b_i$ determines whether there is an edge (a, b), and in case $a_i < b_i$ it is the quadratic residuosity of $i + b_i(b_i - 1)/2 + a_i$ that determines whether the edge (a, b) exists.

Acknowledgments

I would like to thank Noga Alon for fruitful discussions and the anonymous referee, Pete Gemmell and Seffi Naor for carefully reading this manuscript.

References

[1] H. L. Abbot, *A note on Ramsey's theorem*, *Canad. Math. Bull.* **15**, 1972, pp. 9-10.

[2] N. Alon, O. Goldreich, J. Hastad and R. Peralta, *Simple constructions for almost k-wise independent random variables*, *Proc. 31st IEEE Symp. on Foundations of Computer Science*, 1990, pp. 544-553.

[3] N. Alon and J. Spencer, **The probabilistic method**, John Wiley and Sons Inc., New York, 1992.

[4] L. Babai and P. Frankl, *Linear algebra methods in combinatorics, preliminary version*, manuscript, 1988.

[5] P. Erdös, *Some remarks on the theory of graphs*, *Bulletin of the American Mathematics Society* **53**, 292-294, 1947.

[6] P. Frankl, *A constructive lower bound for Ramsey numbers*, *Ars Combinatorica* **3**, 297-302, 1977.

[7] P. Frankl and R. M. Wilson, *Intersection theorems with geometric consequences*, *Combinatorica* **1**, 357-368, 1981.

[8] R. L. Graham, B. L. Rothschild and J. H. Spencer, **Ramsey Theory**, John Wiley and Sons Inc., New York, 1980.

[9] J. Justesen, *A class of constructive asymptotically good algebraic codes, IEEE Trans. Inform. Theory,* IT-18 (1972), 652–656.

[10] F.J. MacWilliams, N.J.A. Sloane, **The Theory of Error-Correcting Codes,** North Holland, Amsterdam, 1977.

[11] J. Naor, M. Naor, *Small-bias probability spaces: efficient constructions and applications, Proc. 22-nd ACM Symp. Theory of Comput.* (1990), 213–223.