

7-23-2015

# Random algebraic construction of extremal graphs

Boris Bukh

*Carnegie Mellon University*, [bbukh@math.cmu.edu](mailto:bbukh@math.cmu.edu)

Follow this and additional works at: <http://repository.cmu.edu/math>

 Part of the [Mathematics Commons](#)

---

## Published In

Bulletin of the London Mathematical Society, accepted.

This Working Paper is brought to you for free and open access by the Mellon College of Science at Research Showcase @ CMU. It has been accepted for inclusion in Department of Mathematical Sciences by an authorized administrator of Research Showcase @ CMU. For more information, please contact [research-showcase@andrew.cmu.edu](mailto:research-showcase@andrew.cmu.edu).

# Random algebraic construction of extremal graphs

Boris Bukh\*

## Abstract

We present a motivated construction of large graphs not containing a given complete bipartite subgraph. The key insight is that the algebraic constructions yield very non-smooth probability distributions.

MSC CLASSES: 05C35, 05D99

## Introduction

A foundational problem in extremal graph theory is Turán’s question: how big can a graph be if it does not contain  $H$  as a subgraph? Let  $\text{ex}(n, H)$  be the maximum number of edges in any  $n$ -vertex  $H$ -free graph. Turán himself [19] determined  $\text{ex}(n, H)$  when  $H$  is a clique: He showed that if  $H = K_r$ , then the maximum is attained by a complete  $(r - 1)$ -partite graph whose parts are as equal as possible (see [1] for six different proofs of this result). Erdős–Stone and Simonovits [8, 7, 17] showed that *for every graph  $H$*  the largest  $H$ -free graph is close (in an appropriate sense) to a complete multipartite graph on  $\chi(H) - 1$  parts, where  $\chi(H)$  is the chromatic number of  $H$ . In particular, the asymptotic formula

$$\text{ex}(n, H) = \left(1 - \frac{1}{\chi(H) - 1}\right) \binom{n}{2} + o(n^2) \quad (1)$$

holds.

It is natural to interpret  $1 - \frac{1}{\chi(H) - 1}$  as the fraction of the total number of edges in the complete graph. When  $\chi(H) \geq 3$ , the fraction is positive and (1) is a satisfactory asymptotics. On the other hand, if  $H$  is bipartite, then  $\chi(H) = 2$ , and the main term in (1) vanishes, leaving a notoriously hard open problem of finding an asymptotics for  $\text{ex}(n, H)$  when  $H$  is bipartite.

In this paper we focus on the best-understood class of bipartite graphs, the complete bipartite graphs. Let  $K_{s,t}$  denote the complete bipartite graph with parts of size  $s$  and  $t$ . The following is a basic upper bound on  $\text{ex}(n, K_{s,t})$ .

**Theorem 1** (Kovári–Sós–Turán). *For each  $s$  and  $t$  there is a constant  $C$  such that  $\text{ex}(n, K_{s,t}) \leq Cn^{2-1/s}$ .*

*Proof.* We let  $C$  be a large constant (to be specified later). Suppose  $G = (V, E)$  is a  $K_{s,t}$ -free graph. It suffices to prove that  $G$  contains a vertex of degree less than  $Cn^{1-1/s}$ , for then we may remove it,

---

\*Department of Mathematical Sciences, Carnegie Mellon University, Pittsburgh, PA 15213, USA. Email: bbukh@math.cmu.edu. Supported in part by U.S. taxpayers through NSF grant DMS-1201380.

and apply the induction on the number of vertices since  $C(n-1)^{2-1/s} + Cn^{1-1/s} \leq Cn^{2-1/s}$ . Assume, for contradiction's sake, that  $\deg(v) \geq Cn^{1-1/s}$  for all  $v \in V$ .

Let  $N$  denote the number of copies  $K_{1,s}$  in  $G$ . We count  $N$  in two different ways. On one hand, denoting by  $\deg(v)$  the degree of  $v \in V$ , we obtain

$$N = \sum_{v \in V} \binom{\deg(v)}{s},$$

the summand being the number of copies of  $K_{1,s}$  with the apex  $v$ . Since  $\deg(v) \geq Cn^{1-1/s}$  for all  $v$  and  $C$  is sufficiently large in terms of  $s$ , we have  $\binom{\deg(v)}{s} \geq (\frac{1}{2}Cn^{1-1/s})^s/s! = 2^{-s}C^s n^{s-1}/s!$  and hence

$$N \geq 2^{-s}C^s n^s/s! \tag{2}$$

On the other hand, if  $\{u_1, \dots, u_s\}$  is any set of  $s$  vertices, then no more than  $t-1$  vertices can be adjacent to all of these  $s$  vertices, as  $G$  is  $K_{s,t}$ -free. Thus

$$N \leq (t-1) \binom{n}{s}. \tag{3}$$

Combining (2) and (3) together with the simple bound  $\binom{n}{s} \leq (t-1)n^s/s!$  yields a contradiction unless  $C \leq 2(t-1)^{1/s}$ .  $\square$

Despite being a sixty-year-old result with a simple proof, the Kóvari–Sós–Turán theorem has been improved only once, by Füredi [10] who improved the bound on the constant  $C$ . Is Kóvari–Sós–Turán bound tight? It is for  $K_{2,2}$ , and  $K_{3,3}$  [6, 5], but no constructions of  $K_{s,s}$ -free graphs with  $\Omega(n^{2-1/s})$  edges are known for any  $s \geq 4$ . There are however constructions [12, 2, 4] of  $K_{s,t}$ -free graphs with  $\Omega(n^{2-1/s})$  edges when  $t$  is much larger than  $s$ . The aim of this paper is to present a new construction that uses both the algebra and probability. The construction is inspired by the construction in [4]. As a motivation, we first explain why the standard probabilistic argument is insufficient.

## Sketch of a probabilistic construction

Our graphs will be bipartite, with  $n$  vertices in each part. We refer to the parts as ‘left’ and ‘right’, and denote them  $L$  and  $R$  respectively.

Set  $p = n^{-1/s}$ . For each pair of vertices  $u \in L$ ,  $v \in R$  declare  $uv$  to be an edge with probability  $p$ , different edges being independent. The expected number of edges in  $G$  is  $pn^2 = n^{2-1/s}$ . As the number of edges in  $G$  is binomially distributed,  $G$  will have at least  $\frac{1}{2}n^{2-1/s}$  edges with probability tending to 1 as  $n \rightarrow \infty$ .

We shall show that  $\Pr[K_{s,t} \subset G] \rightarrow 0$  for a suitably large  $t$ . For a set  $U$  of vertices, let

$$N(U) \stackrel{\text{def}}{=} \{v \in V : uv \text{ is an edge for all } u \in U\}$$

be the common neighborhood of  $U$ .

Let  $U$  be any set of  $s$  vertices. We shall bound  $\Pr[|N(U)| \geq t]$ . If  $U$  is not contained in either  $L$  or  $R$ , then  $N(U) = \emptyset$  and  $\Pr[|N(U)| \geq t] = 0$ . Suppose  $U \subset L$  (the case  $U \subset R$  is symmetric). It

is clear that  $v \in N(U)$  with probability  $p^s = 1/n$  for each  $v \in R$ , and these events are independent for different  $v$ 's. Hence,  $|N(U)|$  is a binomial random variable  $\text{Binom}(n, 1/n)$ . It follows that  $|N(U)|$  is distributed approximately as a Poisson random variable with mean 1, and in particular it can be shown that  $\Pr[|N(U)| \geq t] \leq 1/t!$ .

We can bound the probability that  $G$  contains  $K_{s,t}$  by

$$\Pr[K_{s,t} \subset G] \leq \sum_{\substack{U \subset V \\ |U|=s}} \Pr[|N(U)| \geq t] \leq 2 \binom{n}{s} \frac{1}{t!}.$$

(The two cases  $U \subset L$  and  $U \subset R$  are responsible for the factor of 2.) If  $t = 10s \frac{\log n}{\log \log n}$ , then this probability is very close to 0. Thus with high probability  $G$  contains approximately  $\Theta(n^{2-1/s})$  edges, and contains no  $K_{s,t}$  for  $t = 10s \frac{\log n}{\log \log n}$ .

The analysis above is nearly tight: one can show that for  $t = 0.1s \frac{\log n}{\log \log n}$ , the random graph contains  $K_{s,t}$  with overwhelming probability (see [3, Section 4.5] for a proof of a similar result for cliques).

So, the reason for the failure of probabilistic construction is that while  $|N(U)|$  has mean 1, the distribution of  $|N(U)|$  has a long, smoothly-decaying tail. Since there are many sets  $U$ , it is likely that  $|N(U)|$  is large for some  $U$ .

## Random algebraic construction

Let  $q$  be a prime power, and let  $\mathbb{F}_q$  be the finite field of order  $q$ . We shall assume that  $s \geq 4$  is fixed, and that  $q$  is sufficiently large as a function of  $s$ . Let  $d = s^2 - s + 2$ ,  $n = q^s$ . The graph  $G$  that we will construct in this section will be bipartite. Each of the two parts,  $L$  and  $R$ , will be identified with  $\mathbb{F}_q^s$ .

Suppose  $f$  is a polynomial in  $2s$  variables over  $\mathbb{F}_q$ . We write the polynomial as  $f(X, Y)$  where  $X = (X_1, \dots, X_s)$  and  $Y = (Y_1, \dots, Y_s)$  are the first and the last  $s$  variables respectively. Such a polynomial induces a bipartite graph in the natural way: pair  $(x, y) \in L \times R$  is an edge if  $f(x, y) = 0$ .

Let  $\mathcal{P} \subset \mathbb{F}_q[X, Y]$  be the set of all polynomials of degree at most  $d$  in each of  $X$  and  $Y$ . Pick a polynomial  $f$  uniformly from  $\mathcal{P}$  and let  $G$  be the associated graph. We shall show that  $G$ , on average, contains many edges but hardly any copies of  $K_{s,t}$  for  $t = s^d + 1$ . We will then remove few vertices from  $G$  to render  $G$  completely free of  $K_{s,t}$ 's while still leaving many edges left.

We show that  $G$  behaves very similarly to the random graph that we constructed in the previous section with  $p = 1/q$ . We begin by counting the number of edges in  $G$ .

**Lemma 2.** *For every  $u, v \in \mathbb{F}_q^s$ , we have  $\Pr[f(u, v) = 0] = 1/q$ . In particular, the expected number of edges in  $G$  is  $n^2/q$ .*

*Proof.* Fix  $u, v \in \mathbb{F}_q^s$ . Let  $\mathcal{P}_0 = \{f \in \mathcal{P} : f(0, 0) = 0\}$  be the set of polynomials with zero constant term. Every  $f \in \mathcal{P}$  can be written uniquely as  $f = g + h$ , where  $g \in \mathcal{P}_0$  and  $h$  is a constant. So, a way to sample  $f \in \mathcal{P}$  uniformly is to first sample  $g$  from  $\mathcal{P}_0$ , and then sample  $h$  from  $\mathbb{F}_q$ . It is clear that having chosen  $g$ , out of  $q$  possible choices for  $h$  exactly one choice results in  $f(u, v) = 0$ .  $\square$

To count the copies of  $K_{s,t}$  we shall look at the distribution of  $|N(U)|$ , where  $U$  is an arbitrary set of  $s$  vertices in the same part. We shall focus on the case  $U \subset L$ , the other case being symmetric.

Computing the distribution of  $|N(U)|$  directly is hard. Instead we will compute moments of  $|N(U)|$  with aid of the following two lemmas:

**Lemma 3.** *Suppose  $u, u' \in \mathbb{F}_q^s$  are two distinct points, and  $L$  is a linear function chosen uniformly among all linear functions  $\mathbb{F}_q^s \rightarrow \mathbb{F}_q$ . Then  $\Pr[Lu = Lu'] = 1/q$ .*

*Proof.* Since  $u$  and  $u'$  are distinct, there is a coordinate in which they differ. Without loss of generality, it is the first coordinate. A linear function is uniquely determined by its action on the basis vectors  $e_1, \dots, e_s$ . Sample  $L$  by first sampling  $Le_2, \dots, Le_s$  and then sampling  $Le_1$ . Having chosen  $Le_2, \dots, Le_s$  there is precisely one choice for  $Le_1$  such that  $Lu = Lu'$ .  $\square$

**Lemma 4.** *Suppose  $r, s \leq \min(\sqrt{q}, d)$ . Let  $U \subset \mathbb{F}_q^s$  and  $V \subset \mathbb{F}_q^r$  be sets of size  $s$  and  $r$  respectively. Then*

$$\Pr[f(u, v) = 0 \text{ for all } u \in U, v \in V] = q^{-sr}.$$

*Proof.* Call a set of points in  $\mathbb{F}_q^s$  *simple* if the first coordinates of all the points are distinct.

We first give the proof in the case when  $U$  and  $V$  are simple sets. In this case, we decompose  $f$  as  $f = g + h$ , where  $h$  contains the monomials  $X_1^i Y_1^j$  for  $i = 0, 1, \dots, s-1$  and  $j = 0, 1, \dots, r-1$ , whereas  $g$  contains all the other monomials. Similarly to the proof of the preceding lemmas it is sufficient to show that the system of linear equations

$$h(u, v) = -g(u, v) \quad \text{for all } u \in U, v \in V \tag{4}$$

has a unique solution with polynomial  $h$  as the unknown. This is a consequence of the Lagrange interpolation theorem applied twice: the first application yields, for each  $u \in U$ , single-variate polynomials  $h_u(Y)$  of degree at most  $r-1$  such that  $h_u(v) = -g(u, v)$  for all  $v \in V$ ; the second application yields a polynomial  $h(X, Y)$  such that each if the coefficients of  $h(u, Y)$  is equal to the respective coefficient of  $h_u(Y)$  for all  $u \in U$ . That latter condition implies of course that  $h(u, v) = h_u(v)$ . Note that the obtained polynomial  $h$  is unique since the solution exists for each of  $q^{rs}$  possible right-hand sides in (4), and there are only  $q^{rs}$  polynomials  $h$ .

We next treat the case of general  $U$  and  $V$ . It suffices to find invertible linear transformations  $T$  and  $S$  acting on  $\mathbb{F}_q^s$  such that both  $TU$  and  $SV$  are simple. Indeed, the set of polynomials  $\mathcal{P}$  is invariant under change of coordinates in the first  $s$  coordinates, and is invariant under change of coordinates in the last  $s$  coordinates. Hence, if we arrange for  $TU$  and  $SV$  to be simple, we reduce to the special case treated above.

To find the requisite  $T$ , it suffices to find a linear map  $T_1: \mathbb{F}_q^s \rightarrow \mathbb{F}_q$  that is injective on  $U$ . We can then find an invertible map  $T: \mathbb{F}_q^s \rightarrow \mathbb{F}_q^s$  whose first coordinate is  $T_1$ . We pick  $T_1$  uniformly at random from among all linear maps  $\mathbb{F}_q^s \rightarrow \mathbb{F}_q$ . By lemma 3, for any distinct  $x, x' \in X$ , the probability that  $T_1x = T_1x'$  is  $1/q$ , and so

$$\Pr[\exists x, x' \in X, x \neq x' \wedge T_1x = T_1x'] \leq \binom{s}{2} \frac{1}{q} < 1,$$

implying that a suitable  $T_1$  (and hence  $T$ ) exists. The construction of  $S$  is analogous.  $\square$

Fix a set  $U \subset \mathbb{F}_q^s$  of size  $s$ . For  $v \in \mathbb{F}_q^s$ , put  $I(v) = 1$  if  $f(u, v) = 0$  for all  $u \in U$ , and  $I(v) = 0$  if  $f(u, v) \neq 0$  for some  $u \in U$ . The  $d$ 'th moment of  $|N(U)|$  is easily computed by writing  $|N(U)|$  as a sum of  $I(v)$ 's and expanding:

$$\begin{aligned} \mathbb{E}[|N(U)|^d] &= \mathbb{E}\left[\left(\sum_{v \in \mathbb{F}_q^s} I(v)\right)^d\right] = \mathbb{E}\left[\sum_{v_1, \dots, v_d \in \mathbb{F}_q^s} I(v_1)I(v_2) \cdots I(v_d)\right] \\ &= \sum_{v_1, \dots, v_d \in \mathbb{F}_q^s} \mathbb{E}[I(v_1)I(v_2) \cdots I(v_d)] \end{aligned}$$

The preceding lemma tells us that the summand is equal to  $q^{-rs}$  if there are exactly  $r$  distinct points among  $v_1, \dots, v_d$ . Let  $M_r$  be the number of surjective functions from a  $d$ -element set onto an  $r$ -element set, and let  $M = \sum_{r \leq d} M_r$ . Breaking the sum according to the number of distinct elements among  $v_1, \dots, v_d$ , we see that

$$\mathbb{E}[|N(U)|^d] = \sum_{r \leq d} \binom{q^s}{r} M_r q^{-rs} \leq \sum_{r \leq d} M_r = M.$$

We can use the moments to bound the probability that  $|N(U)|$  is large:

$$\Pr[|N(U)| \geq \lambda] = \Pr[|N(U)|^d \geq \lambda^d] \leq \frac{\mathbb{E}[|N(U)|^d]}{\lambda^d} \leq \frac{M}{\lambda^d}. \quad (5)$$

We have shown that distribution of edges of  $G$  enjoys some independence, and used that to derive (5). It is now time to exploit the dependence between the edges of  $G$ . The following result provides severe constraints on the values attainable by  $|N(U)|$ :

**Lemma 5.** *For every  $s$  and  $d$  there exists a constant  $C$  such the following holds: Suppose  $f_1(Y), \dots, f_s(Y)$  are  $s$  polynomials on  $\mathbb{F}_q^s$  of degree at most  $d$ , and consider the set*

$$W = \{y \in \mathbb{F}_q^s : f_1(y) = \cdots = f_s(y) = 0\}.$$

*Then exactly one of the following holds:*

1. *(Zero-dimensional case)  $|W| \leq C$ ,*
2. *(Higher-dimensional case)  $|W| \geq q - C\sqrt{q}$ .*

*The constant  $C$  depends only on  $s$  and the degrees of  $f$ 's.*

*Proof.* The proof of this lemma is the sole place in the paper where we use algebraic geometry. A basic textbook is [16]. For technical reasons, we will work not with projective, but with affine varieties, and so the intersection theory that we will employ differs slightly from the most common sources. Namely, we will use the results from [11]. In particular, we use the same notion of the degree of a variety, namely  $\deg V = \sum \deg V_i$ , where the sum is over irreducible components of  $V$ . The notion obeys the familiar properties: First, the degree of the variety  $\{f = 0\}$ , where  $f$  is a non-zero polynomial, is at most  $\deg f$ . Second, if  $X$  is a zero-dimensional variety, then  $\deg X$  is just the number of points in  $X$ .

Finally, in Theorem 1 on page 251 of the same paper, it is shown that the Bezout's inequality holds, namely

$$\deg X \cap Y \leq \deg X \cdot \deg Y,$$

for any two varieties  $X, Y$ . (A similar result in the projective space can be found in [9, Example 12.3.1].)

By dimension of a variety defined over a finite field  $\mathbb{F}_q$ , we will mean the dimension of the variety as a variety over the algebraic closure  $\overline{\mathbb{F}_q}$  (see [16, Chapter 6]).

To establish the lemma it suffices to prove that, for any fixed  $m$  and  $D$ , whenever  $V$  is an (affine) variety defined over  $\mathbb{F}_q$  of degree  $D$  and dimension  $m$ , then the set of  $\mathbb{F}_q$ -points of  $V$  satisfies either  $|V(\mathbb{F}_q)| = O(1)$  or  $|V(\mathbb{F}_q)| \geq q - O(\sqrt{q})$ . Indeed,  $W$  is the set of  $\mathbb{F}_q$ -points of the variety with equations  $f_1 = \dots = f_s = 0$ , and its degree is bounded by Bezout's inequality applied to the varieties  $\{f_i = 0\}$ . Here "bounded" means bounded in terms of  $m$  and  $D$ ; similarly, the constants in the big-oh notation are allowed to depend on  $m$  and  $D$ .

The proof is by induction on  $m$  (for all  $D$  simultaneously). In the base case  $m = 0$  is trivial, as we then have  $|V| = D$ . Suppose  $m \geq 1$ . If  $V$  is reducible over  $\mathbb{F}_q$ , then the degrees of the components add up to  $D$ , and we can treat each component separately. So, assume that  $V$  is irreducible over  $\mathbb{F}_q$ . If  $V$  is also irreducible over  $\overline{\mathbb{F}_q}$  then it has  $q^{\dim V}(1 - O(1/\sqrt{q}))$  points by the Lang–Weil bound [13] (for an elementary proof see [15]). Otherwise  $V$  is reducible over  $\overline{\mathbb{F}_q}$ , with  $V_1, \dots, V_r$  as the components. The reducibility means that  $r \geq 2$ . The Frobenius automorphism  $x \mapsto x^q$  acts on  $V$ , permuting the components. The action is transitive because  $V$  is irreducible over  $\mathbb{F}_q$ . Indeed, if  $V_1, \dots, V_l$  is an orbit of the action, then the variety  $V_1 \cup \dots \cup V_l$  is invariant under the action of the Frobenius automorphism, and so is  $\mathbb{F}_q$ -definable [18, Proof of Corollary 4]. Similarly, each orbit gives rise to a proper subvariety of  $V$ . As the union of these subvarieties is  $V$ , this contradicts the irreducibility of  $V$ . The contradiction shows that the action is transitive, as claimed.

Let  $V' = V_1 \cap \dots \cap V_r$ . In view of the transitivity we have  $V_1(\mathbb{F}_q) = \dots = V_r(\mathbb{F}_q)$ , and so  $V(\mathbb{F}_q) = V'(\mathbb{F}_q)$ . As  $V'$  is invariant under the action of the Frobenius automorphism, it is  $\mathbb{F}_q$ -definable. As  $V$  is irreducible over  $\mathbb{F}_q$ , we cannot have  $\dim V' = \dim V$  for it would follow that  $V = V'$ , contrary to  $r \geq 2$ . Hence,  $\dim V' < \dim V = m$ . Moreover, we can bound the degree of  $V'$  via Bezout's inequality as follows

$$\deg V' \leq \prod \deg V_i \leq \left(\frac{1}{r} \sum \deg V_i\right)^r = (D/r)^r \leq \exp(D/e).$$

Since  $V(\mathbb{F}_q) = V'(\mathbb{F}_q)$ , the result follows from the induction hypothesis.  $\square$

We consider  $s$  polynomials  $f(u, \cdot)$  as  $u$  ranges over  $U$ . The preceding lemma then says that either  $|N(U)| \leq C$  or  $|N(U)| \geq q/2$  if  $q$  is sufficiently large in terms of  $s$ . From (5) we thus obtain (for all sufficiently large  $q$ )

$$\Pr[|N(U)| > C] = \Pr[|N(U)| \geq q/2] \leq \frac{M}{(q/2)^d}.$$

Call a set of  $s$  vertices of  $G$  *bad* if their common neighborhood has more than  $C$  vertices. Let  $B$  the number of bad sets. The above shows that

$$\mathbb{E}[B] \leq 2 \binom{n}{s} \frac{M}{(q/2)^d} = O(q^{s-2}). \quad (6)$$

Remove a vertex from each bad set counted by  $B$  from  $G$  to obtain graph  $G'$ . Since no vertex has degree more than  $q^s$ , the number of edges in  $G'$  is at most  $Bq^s$  fewer than in  $G$ . Hence, the expected number of edges in  $G'$  is at least

$$n^2/q - \mathbb{E}[B]q^s = \Omega(n^{2-1/s}),$$

where  $n^2/q$  comes from Lemma 2, and the estimation of  $\mathbb{E}[B]$  comes from (6).

Therefore, there exists a graph with at most  $2n$  vertices and  $\Omega(n^{2-1/s})$  edges, but without  $K_{s,C+1}$ .

*Remark.* An earlier version of this paper asserted that the constant  $C$  in Lemma 5 can be taken to be  $\prod \deg f_i$ . The assertion is false. Here is an example based on the idea of Jacob Tsimerman. Let  $a$  be any element of  $\mathbb{F}_{p^2}$  that is not in  $\mathbb{F}_p$ , and choose univariate polynomials  $g$  and  $h$  of degrees  $d$  and  $d-1$  respectively that are completely reducible over  $\mathbb{F}_p$  with distinct roots. The bivariate polynomial  $ag(x) + h(y)$  is irreducible over  $\overline{\mathbb{F}_p}$ . Indeed, if it were reducible, then its Newton polygon<sup>1</sup> would be a Minkowski sum of Newton polygons of its factors [14, Theorem VI]. Since  $\{(d, 0), (0, d-1)\}$  is not a Minkowski sum of two smaller lattice polygons,  $ag(x) + h(y)$  is irreducible over  $\overline{\mathbb{F}_p}$ . Polynomial  $a^p g(x) + h(y)$  is similarly irreducible. Let  $f_1(x, y, z) = (ag(x) + h(y))(a^p g(x) + h(y))$ . Since  $f_1$  is invariant under the Frobenius automorphism,  $f_1 \in \mathbb{F}_p[x, y, z]$ . Let  $f_2(x, y, z) = f_3(x, y, z) = z$ . Then common zero set of  $f_1, f_2, f_3$  is the set  $\{(x, y, z) : g(x) = h(y) = z = 0\}$  which has size  $d(d-1)$ , whereas  $\prod \deg f_i = 2d$ .

**Acknowledgements.** I am grateful to Roman Karasev for valuable discussions, and to David Conlon, Zilin Jiang, and Eoin Patrick Long for comments on the earlier versions of this paper. I also thank the anonymous referee for detailed feedback and pointing reference [11].

## References

- [1] Martin Aigner. Turán's graph theorem. *Amer. Math. Monthly*, 102(9):808–816, 1995.
- [2] Noga Alon, Lajos Rónyai, and Tibor Szabó. Norm-graphs: variations and applications. *J. Combin. Theory Ser. B*, 76(2):280–290, 1999.
- [3] Noga Alon and Joel H. Spencer. *The probabilistic method*. Wiley-Interscience Series in Discrete Mathematics and Optimization. Wiley-Interscience [John Wiley & Sons], New York, second edition, 2000. With an appendix on the life and work of Paul Erdős.
- [4] Pavle V. M. Blagojević, Boris Bukh, and Roman Karasev. Turán numbers for  $K_{s,t}$ -free graphs: topological obstructions and algebraic constructions. *Israel J. Math.*, 197(1):199–214, 2013.
- [5] W. G. Brown. On graphs that do not contain a Thomsen graph. *Canad. Math. Bull.*, 9:281–285, 1966.
- [6] P. Erdős, A. Rényi, and V. T. Sós. On a problem of graph theory. *Studia Sci. Math. Hungar.*, 1:215–235, 1966.

---

<sup>1</sup>Newton polygon of a bivariate polynomial  $\sum_{i,j} a_{i,j} x^i y^j$  is the convex hull of  $\{(i, j) : a_{i,j} \neq 0\}$ .



- [7] P. Erdős and M. Simonovits. A limit theorem in graph theory. *Studia Sci. Math. Hungar.*, 1:51–57, 1966.
- [8] P. Erdős and A. H. Stone. On the structure of linear graphs. *Bull. Amer. Math. Soc.*, 52:1087–1091, 1946.
- [9] William Fulton. *Intersection theory*, volume 2 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]*. Springer-Verlag, Berlin, second edition, 1998.
- [10] Zoltán Füredi. An upper bound on Zarankiewicz’ problem. *Combin. Probab. Comput.*, 5(1):29–33, 1996.
- [11] Joos Heintz. Definability and fast quantifier elimination in algebraically closed fields. *Theoret. Comput. Sci.*, 24(3):239–277, 1983. Also corrigendum in vol. 39 (1985), no. 2-3, 343.
- [12] János Kollár, Lajos Rónyai, and Tibor Szabó. Norm-graphs and bipartite Turán numbers. *Combinatorica*, 16(3):399–406, 1996.
- [13] Serge Lang and André Weil. Number of points of varieties in finite fields. *Amer. J. Math.*, 76:819–827, 1954.
- [14] A. M. Ostrowski. On multiplication and factorization of polynomials. I. Lexicographic orderings and extreme aggregates of terms. *Aequationes Math.*, 13(3):201–228, 1975.
- [15] Wolfgang M. Schmidt. *Equations over finite fields. An elementary approach*. Lecture Notes in Mathematics, Vol. 536. Springer-Verlag, Berlin-New York, 1976.
- [16] I. R. Shafarevich. *Basic algebraic geometry*. Springer-Verlag, New York-Heidelberg, 1974. Translated from the Russian by K. A. Hirsch, Die Grundlehren der mathematischen Wissenschaften, Band 213.
- [17] M. Simonovits. A method for solving extremal problems in graph theory, stability problems. In *Theory of Graphs (Proc. Colloq., Tihany, 1966)*, pages 279–319. Academic Press, New York, 1968.
- [18] Terence Tao. Lang–Weil bound (blog post). <http://terrytao.wordpress.com/2012/08/31/the-lang-weil>
- [19] P. Turán. On an extremal problem in graph theory (in Hungarian). *Math. Fiz. Lapok*, 48:436–452, 1941.