# A QUASI-RANDOM GRAPH SEQUENCE

MILES KRETSCHMER

Fix a prime $p$. Let $q = p^r$ be a power of $p$, and $F_q$ the field with $q$ elements. We let $F_q^+$ denote its additive group and $F_q^\times$ its multiplicative group. We then have the Artin-Schreier homomorphism

$$\tau : F_q^+ \to F_q^+$$
$$t \mapsto t^p - t$$

This fits into an exact sequence

$$0 \longrightarrow F_p^+ \longrightarrow F_q^+ \xrightarrow{\tau} F_q^+ \longrightarrow F_q^+/\tau F_q^+ \longrightarrow 0$$

Therefore, $\left[F_q^+ : \tau F_q^+\right] = p$. We form a graph $G_q$ with vertex set $F_q$, connecting $x \neq y$ by an edge if $x \cdot y \in \tau F_q^+$. For $x \in F_q^\times$, $x$ is connected to exactly those $y \in x^{-1}\tau F_q^+$ which are not equal to $x$. As multiplication by $x^{-1}$ is an automorphism of $F_q^+$, this is also a subgroup of index $p$. Thus the neighborhood $N(x)$ of $x$ has size $q/p$ or $q/p - 1$.

**Theorem 1.** *The sequence of graphs $G_q$ for $q = p^r$, $r$ a natural number, is quasi-random with edge density $1/p$.*

*Proof.* We use the following criterion. For $x, y$ vertices, let $n(x, y) = |N(x) \cap N(y)|$. It then suffices to show that

$$\sum_{x,y} \left| n(x, y) - \frac{q}{p^2} \right| = o(q^3)$$

We will in fact show that this sum is bounded by a constant multiple of $q^2$. We first replace $n(x, y)$ with a quantity that is easier to count. Let $N^\star(x)$ be $x^{-1}\tau F_q^+$ if $x \in F_q^\times$, and $F_q$ if $x = 0$. This differs from $N(x)$ only in that it may contain $x$. We define

$$n^\star(x, y) = |N^\star(x) \cap N^\star(y)|$$

Now $|n^\star(x, y) - n(x, y)| \leq 2$, so

$$\sum_{x,y} \left| n(x, y) - \frac{q}{p^2} \right| \leq \sum_{x,y} \left| n^\star(x, y) - \frac{q}{p^2} \right| + 2q^2$$

Therefore, it suffices to bound the latter quantity by a constant multiple of $q^2$.

Now, note that $N^\star(x) \cap N^\star(y)$ is either

(1) all of $F_q$, if $x = y = 0$
(2) a subgroup of index $p$, if one of $x$ and $y$ is nonzero and the other is 0
(3) an intersection of two subgroups of index $p$, if $x$ and $y$ are both nonzero

We see that in each case, $n^\star(x, y) \geq q/p^2$. Therefore, we can get rid of the absolute value in the sum, and bound the quantity

$$\sum_{x,y} n^\star(x, y) - \frac{q^3}{p^2}$$

The sum

$$\sum_{x,y} n^\star(x, y)$$

*Date*: August 2024.

is the number of triples $(x, y, z)$ such that $xz \in \tau F_q^+$ and $yz \in \tau F_q^+$. We will count these triples by counting the number of 5-tuples in the set

$$S = \{(x, y, z, s, t) \in F_q^5 \mid xz = t^p - t \text{ and } yz = s^p - s\}$$

Each triple $(x, y, z)$ then corresponds to $p^2$ 5-tuples in $S$, as the fibers of $\tau$ have size $p$. Consequently,

$$\sum_{x,y} n^\star(x, y) = \frac{|S|}{p^2}$$

To count the number of elements in $S$, we let

$$S_z = \{(x, y, s, t) \in F_q^4 \mid (x, y, z, s, t) \in S\}$$

For $z = 0$ we have $S_0 = F_q \times F_q \times F_p \times F_p$, so $|S_0| = q^2p^2$. For $z \in F_q^\times$, a choice $(x, y, s, t) \in S_z$ is determined by any choice of $(s, t)$, so $|S_z| = q^2$ in this case. Summing over all $z$, we have

$$|S| = q^2p^2 + (q - 1)q^2$$

Therefore,

$$\frac{|S|}{p^2} = q^2 + \frac{(q-1)q^2}{p^2} = \left[1 - \frac{1}{p^2}\right] q^2 + \frac{q^3}{p^2}$$

and so

$$\sum_{x,y} \left| n^\star(x, y) - \frac{q}{p^2} \right| = \sum_{x,y} n^\star(x, y) - \frac{q^3}{p^2} = \left[1 - \frac{1}{p^2}\right] q^2$$

which is a constant multiple of $q^2$, as required. We conclude that the graph sequence $\{G_q\}$ is quasi-random with edge density $\frac{1}{p}$. □

> "When you observe an interesting property of numbers, ask if perhaps you are not seeing, in the $1 \times 1$ case, an interesting property of matrices" -Olga Taussky

Indeed, we can generalize this to matrices over finite fields. We define $G_q^n$ to be a graph whose vertex set is $\mathrm{M}_n(F_q)$, the set of $n \times n$ matrices over $F_q$, where we connect $a \neq b$ by an edge if $\mathrm{tr}(ab) \in \tau F_q^+$. Note that this is a symmetric relation by properties of trace, despite multiplication being non-commutative.

**Theorem 2.** *For fixed $n$, the sequence of graphs $G_q^n$ for $q = p^r$, $r$ ranging over natural numbers, is quasi-random with edge density $1/p$.*

Note that the previous theorem is the $n = 1$ case.

*Proof.* The strategy is similar to the previous proof. The trace map is a surjective abelian group homomorphism

$$\mathrm{tr} : \mathrm{M}_n(F_q) \to F_q^+$$

Therefore $(\mathrm{tr})^{-1}(\tau F_q^+)$ is an additive subgroup of $\mathrm{M}_n(F_q)$ of index $p$. We denote this subgroup by $H$. We will show as before that

$$\sum_{a,b} \left| n(a, b) - \frac{q^{n^2}}{p^2} \right| = o(q^{3n^2})$$

We define, in a similar way as before

$$N^\star(a) = \{b \in \mathrm{M}_n(F_q) \mid ab \in H\}$$

$$n^\star(a, b) = |N^\star(a) \cap N^\star(b)|$$

Again we have

$$\sum_{a,b} \left| n(a, b) - \frac{q}{p^2} \right| \leq \sum_{a,b} \left| n^\star(a, b) - \frac{q^{n^2}}{p^2} \right| + 2q^{2n^2}$$

so it suffices to bound this latter sum. $N^\star(a)$ is the preimage of $H$ under the endomorphism of the additive group $\mathrm{M}_n(F_q)$ given by left multiplication by $a$, so is a subgroup of index at most $p$. Therefore $N^\star(a) \cap N^\star(b)$

is the intersection of two subgroups of index at most $p$, so a subgroup of index at most $p^2$. Thus $n^\star(a,b) \geq q^{n^2}/p^2$. We can therefore remove the absolute value signs, and bound

$$\sum_{a,b} n^\star(a,b) - \frac{q^{3n^2}}{p^2}$$

As before, the sum is the number of triples $(a,b,c)$ such that $ac \in H$ and $bc \in H$. Let $T$ be the set of such triples. We let

$$T_c = \{(a,b) \in \mathrm{M}_n(F_q) \times \mathrm{M}_n(F_q) \mid (a,b,c) \in T\}$$

For $c \in \mathrm{GL}_n(F_q)$, $T_c = Hc^{-1} \times Hc^{-1}$, the Cartesian product of two copies of the image of $H$ under right multiplication by $c^{-1}$. Therefore, $|T_c| = q^{2n^2}/p^2$ in this case.

For $c \notin \mathrm{GL}_n(F_q)$, we have in any case that $|T_c| \leq q^{2n^2}$. We will now bound the size of the set of singular matrices

$$\mathrm{M}_n(F_q) \setminus \mathrm{GL}_n(F_q)$$

A matrix is in this set if either its first column is 0, or its first column is nonzero and its second column is a scalar multiple of its first, or its first two columns are linearly independent and its third is a linear combination of them, etc. This gives a rough bound

$$\begin{aligned}|\mathrm{M}_n(F_q) \setminus \mathrm{GL}_n(F_q)| &\leq q^{n(n-1)} + q \cdot q^{n(n-1)} + q^2 \cdot q^{n(n-1)} + \cdots + q^{n-1} \cdot q^{n(n-1)} \\ &\leq n \cdot q^{n-1} \cdot q^{n(n-1)} = n \cdot q^{n^2-1}\end{aligned}$$

Together with the fact that $|\mathrm{GL}_n(F_q)| \leq q^{n^2}$, we have the bound

$$|T| = \sum_c |T_c| \leq q^{n^2} \cdot \frac{q^{2n^2}}{p^2} + n \cdot q^{n^2-1} \cdot q^{2n^2} = \frac{q^{3n^2}}{p^2} + n \cdot q^{3n^2-1}$$

And therefore,

$$\begin{aligned}\sum_{a,b} \left| n(a,b) - \frac{q^{n^2}}{p^2} \right| &\leq \sum_{a,b} \left| n^\star(a,b) - \frac{q^{n^2}}{p^2} \right| + 2q^{2n^2} = \sum_{a,b} n^\star(a,b) - \frac{q^{3n^2}}{p^2} + 2q^{2n^2} = |T| - \frac{q^{3n^2}}{p^2} + 2q^{2n^2} \\ &\leq n \cdot q^{3n^2-1} + 2q^{2n^2} = o(q^{3n^2})\end{aligned}$$

as required. We conclude that for fixed $n$, $\{G_q^n\}$ is quasi-random with edge density $1/p$.

$\square$