

Counting Cliques in Finite Distant Graphs

Tim Silverman

Abstract

We state and prove some counting formulas relating to cliques in the distant graphs of projective lines over finite rings. As a preliminary to this, we prove a decomposition theorem for the graphs in terms of the direct-product decomposition of their rings.

Keywords: Projective line over a ring; distant graph; q-binomial coefficient.

1 Introduction

A projective line over a ring can be made into a graph, the **distant graph**, where the vertices are the points of the projective line, and where an edge exists between two vertices when the points are “distant” (for which, see below). In [9] (for the commutative case) and [10] (for the noncommutative case) there are tabulated certain vital statistics relating to the counts of cliques in distant graphs over finite rings of small order (up to 32). However, these papers omit to mention that there exist polynomial formulas for these vital statistics, in terms of the sizes of various objects associated with the rings. In this paper, we derive and discuss these formulas.

In Section 1, we recapitulate existing material on the distant graphs of projective lines over general rings and derive certain general results that we will use in subsequent sections. From the point of view of later sections, the most useful result in this section is our decomposition theorem, Proposition 1.3, which asserts that the distant graph of a direct product of rings is the tensor product of the distant graphs of the direct factors.

In Section 2, we derive formulas for the commutative case, and in Section 3 for the general case. In Section 4 we exhibit a relationship between some coefficients of our counting polynomials and some other, better known, coefficients related to partitions. Some incidental extras appear in the appendices.

We introduce graphs first. A **simple** graph is an undirected graph with no multiple edges or self loops (we do not assume here that the vertex set is finite). Each graph we shall be dealing with will be *either* a simple graph, *or* the graph with one vertex and a single loop, which we shall call T . (The presence of this odd exception will, we hope, appear less *ad hoc* later on.) Given two vertices a_1 and a_2 , let us write $a_1 \sim a_2$ if there is an edge between them (or $a_1 \underset{A}{\sim} a_2$ if we need to specify the graph A). A map between graphs is a map f of the underlying sets such that $a_1 \sim a_2 \Rightarrow f(a_1) \sim f(a_2)$. Among the various ways to define a product of graphs, the one we are interested in here is the so-called **tensor product**: the vertex set of the tensor product $A \times B$ is the cartesian product of the vertex sets of A and B , and $\langle a_1, b_1 \rangle_{A \times B} \underset{A \times B}{\sim} \langle a_2, b_2 \rangle \Leftrightarrow a_1 \underset{A}{\sim} a_2$ and $b_1 \underset{B}{\sim} b_2$.

Remark 1.1. Since there are no loops (except in T), no map of graphs can send two adjacent vertices of a graph to the same vertex of its image (unless the image is T). The loop also prevents there from being any maps out of T (other than the identity).

Now we bring in rings. Let R be a ring with identity. Over this, we can construct the ring of 2×2 matrices, $M_2(R)$, and sitting inside this is $GL_2(R)$, the group of invertible 2×2 matrices. Let $GL_2(R)$ act on R^2 from the right. Sitting inside R^2 are free modules of rank 1, and, among these, the modules which also have a free rank 1 complement, such as $R(1, 0)$, form a single orbit under the action of $GL_2(R)$. We say that this orbit is the set of points of the **projective line** over R , $\mathbb{P}(R)$ (see Section 2 of [2]). Each point in $\mathbb{P}(R)$ is of the form $R(a, b)$ for some (a, b) , *viz.* the image of $(1, 0)$ under some element of $GL_2(R)$ of the form $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Such a pair (a, b) is called **admissible**. Every admissible pair is *unimodular*, that is $\exists x, \exists y : ax + by = 1$.

Proposition 1.2. *Two admissible pairs (a, b) and (a', b') generate the same point iff there is a unit u with $(a, b) = u(a', b')$.*

Proof. This combines parts 1 and 2 of Proposition 2.1 of [2]. \square

Since $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \mathrm{GL}_2(R)$, one of the points of $\mathbb{P}(R)$ is $R(0, 1)$. Consider the images of the pair $\langle R(1, 0), R(0, 1) \rangle$ under an element of $\mathrm{GL}_2(R)$. The elements of such pairs are said to be **distant** from each other, and distantness gives a graph structure on the points of $\mathbb{P}(R)$, on which $\mathrm{GL}_2(R)$ acts as graph automorphisms. If p and q are mutually distant, we write $\mathbf{p} \triangle \mathbf{q}$. Note that admissible pairs (a, b) and (c, d) generate mutually distant points just when $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(R)$.

Now, a ring homomorphism $f : R \rightarrow S$ gives rise to a homomorphism of the corresponding matrix rings $\mathrm{M}_2(R) \rightarrow \mathrm{M}_2(S)$ via $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \rightarrow \begin{pmatrix} a^f & b^f \\ c^f & d^f \end{pmatrix}$, and this gives rise to a group homomorphism $\mathrm{GL}_2(R) \rightarrow \mathrm{GL}_2(S)$. Likewise, there is an induced module homomorphism from R^2 to S^2 which sends a point of $\mathbb{P}(R)$ to some submodule of S^2 . Let a point of $\mathbb{P}(R)$ be of the form $R(a, b)$ for some admissible (a, b) . Then the image of $R(a, b)$ will lie in the submodule $S(a^f, b^f)$, and (a^f, b^f) is itself admissible, being the image of $(1, 0) \in S^2$ under the action of $\begin{pmatrix} a^f & b^f \\ c^f & d^f \end{pmatrix} \in \mathrm{GL}_2(S)$, so we get a map from the points of $\mathbb{P}(R)$ to the points of $\mathbb{P}(S)$. Moreover (Proposition 3.1 of [2]), this map preserves the graph structure. For if $R(a, b) \triangle R(c, d)$ then there is an element $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(R)$.

Then there is an element $\begin{pmatrix} a^f & b^f \\ c^f & d^f \end{pmatrix} \in \mathrm{GL}_2(S)$, so $S(a^f, b^f) \triangle S(c^f, d^f)$. Finally, the action of $\mathrm{GL}_2(R)$ on $\mathbb{P}(R)$ is carried to an action of $\mathrm{GL}_2(S)$ on $\mathbb{P}(S)$. The image of $\mathrm{GL}_2(R)$ in the group of automorphisms of the graph is (by definition, but in agreement with the already-defined case where R is a field) $\mathrm{PGL}_2(R)$.

Note that the trivial ring is sent to the one-vertex, one-loop graph T . The exceptional property of the trivial ring, $1 = 0$, is precisely the reason why $(1, 0) = (0, 1)$ in the free rank-2 module over the trivial ring, which is in turn the reason why the single vertex of its projective line has the exceptional property of being adjacent to itself. And that is why we want T despite its oddity.

Proposition 1.3. *Let R_1 and R_2 be rings and $R_1 \times R_2$ be their direct product. Then $\mathbb{P}(R_1 \times R_2) = \mathbb{P}(R_1) \times \mathbb{P}(R_2)$. That is, (finite) direct products of rings give rise to tensor products of graphs.*

Proof. Let $R \cong R_1 \times R_2$. Then $\mathrm{M}_2(R) \cong \mathrm{M}_2(R_1) \times \mathrm{M}_2(R_2)$ and $\mathrm{GL}_2(R) \cong \mathrm{GL}_2(R_1) \times \mathrm{GL}_2(R_2)$. (This simple but crucial point is made in a more general context in section 2 of [6]). Now, the points of the $\mathbb{P}(R)$ are of the form $R(a, b)$ where (a, b) is admissible. But let $a = \langle a_1, a_2 \rangle$ and $b = \langle b_1, b_2 \rangle$ for $a_1, b_1 \in R_1$ and $a_2, b_2 \in R_2$. Then (a, b) is admissible precisely when (a_1, b_1) and (a_2, b_2) are admissible. For $\exists c, d \in R$ such that $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(R)$ precisely when $\exists c_1, d_1 \in R_1, \exists c_2, d_2 \in R_2$ such that $\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \in \mathrm{GL}_2(R_1)$ and $\begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \in \mathrm{GL}_2(R_2)$. So $\mathbb{P}(R) \cong \mathbb{P}(R_1) \times \mathbb{P}(R_2)$ as a set. Moreover, the same argument proves that $(a, b) \triangle (c, d)$ precisely when $(a_1, b_1) \triangle (c_1, d_1)$ and $(a_2, b_2) \triangle (c_2, d_2)$, so that $\mathbb{P}(R) \cong \mathbb{P}(R_1) \times \mathbb{P}(R_2)$ as a graph. Moreover $\mathrm{GL}_2(R) \cong \mathrm{GL}_2(R_1) \times \mathrm{GL}_2(R_2)$, with each factor of the group acting on the corresponding factor of the product graph. \square

Finite direct products of rings are the same as finite direct sums, so we need not distinguish them in future sections.

Remark 1.4. In the language of category theory, the discussion immediately prior to Proposition 1.3 implies that taking the projective line over a ring is a functor from the category of unital rings to the category whose objects are simple graphs and T , and whose morphisms are graph homomorphisms. (It is not usual to throw T in with simple graphs, but it does no harm.) Moreover, Proposition

1.3 (relating the respective categorical products), together with the trivial ring being sent to T (both being terminal), implies that this functor preserves all finite products. (Indeed on some subcategories, e.g. finite commutative rings, it can be shown to preserve all finite limits.)

2 Counting formulas: the commutative case

Every finite commutative ring is the direct sum of local rings, so, by Proposition 1.3, every distant graph over a finite commutative ring is the tensor product of the distant graphs over local rings; hence our chief task is to characterise the latter. A little algebra shows that (even in the most general case) the condition for $R(1,0) \triangle R(a,b)$, i.e. for $\begin{pmatrix} 1 & 0 \\ a & b \end{pmatrix}$ to be invertible, is just that b should be a unit, and without loss of generality we can assume that $b = 1$. Likewise $R(a,1) \triangle R(b,1)$ just when $a - b$ is a unit. But this requirement takes particularly simple form in a local ring, where it says that a and b lie in different cosets of the maximal ideal. We can now conveniently describe the distant graph of a local ring in terms of its complement. We use vertical bars to denote cardinalities.

Proposition 2.1. *The distant graph of a finite local ring R with Jacobson radical J consists of the complement of the disjoint union of $\frac{|R|}{|J|} + 1$ copies of the complete graph on $|J|$ vertices.*

Proof. Let R be a local ring and let its maximal ideal be J . Every point of $\mathbb{P}(R)$ can be generated by an admissible pair of one of the forms $(a, 1)$ or $(1, a)$. If a point is generated by an admissible pair both of whose components are units (i.e. it can be represented by both forms), let us represent it with the first form; thus we have one point generated by each pair of the form $(r, 1)$ for $r \in R$, and one point generated by each pair of the form $(1, a)$, $a \in J$.

Now, two points of the first form, $(a, 1)$ and $(b, 1)$, are distant just if a and b lie in different cosets of J , or, to put it another way, each coset of J gives a complete graph of order $|J|$ in the complementary graph. Points represented by the second form are all distant to those with the first form, because $\begin{pmatrix} a & 1 \\ 1 & b \end{pmatrix}$ with $b \in J$ has as determinant the sum of 1 and an element of J , and is therefore invertible. But they are non-distant to each other, because $\begin{pmatrix} 1 & a \\ 1 & b \end{pmatrix}$ with $a, b \in J$ has as determinant an element of J , so is not invertible. Hence the set of such elements forms one more complete subgraph of order $|J|$ in the complementary graph. \square

Note that this graph structure depends only on the cardinalities $|R|$ and $|J|$ and not on any other details of the ring structure. Since we are dealing with finite local commutative rings, we can say a little more about the cardinalities. From Theorem 2 of [8], there must be a prime number p and two positive integers n and r such that $|R| = p^{nr}$ and $|J| = p^{(n-1)r}$. Conversely, there is at least one such ring for any choice of p , n , and r , namely the Galois ring (see the remarks near the beginning of section 3 of [8]). Hence all graphs of the appropriate form correspond to some finite commutative ring.

Proposition 2.2. *Let R be a finite commutative ring with identity, and let R_i be its local summands, of order $|R_i|$. Let the corresponding Jacobson radicals be J of order $|J|$ and J_i , of order $|J_i|$, and let $q_i = \frac{|R_i|}{|J_i|}$. Then the following hold.*

- a) *The number of k -cliques in $\mathbb{P}(R)$ is $|J|^k \prod_i \binom{q_i + 1}{k}$.*
- b) *The number of $(k + 1)$ -cliques containing a given k -clique is $|J| \prod_i (q_i + 1 - k)$.*
- c) *The maximal order of a clique is $\min(q_i) + 1$.*

Proof. Consider one of the local rings R_i . From Proposition 2.1, the complement of its distant graph consists of $q_i + 1$ copies of the complete graph on $|J_i|$ vertices. A clique in the distant graph then contains at most one point from any of the complete graphs. Thus there are $|J_i|^k \binom{q_i + 1}{k}$ k -cliques altogether; and the number of $(k + 1)$ -cliques containing a given k -clique is $|J_i| (q_i + 1 - k)$.

k points of a product graph are mutually distant precisely when their components in each factor are mutually distant, so the number of k -cliques in the projective line over a finite ring is just the product of the number in each local summand ring. Since J is the cartesian product of the J_i , $|J| = \prod_i |J_i|$, the cardinality $|J|$ can be pulled out of the product to give the formulas stated above.

When $k = q_i + 1$, obviously $|J_i| (q_i + 1 - k) = 0$, so $q_i + 1$ is the maximal order of a clique in R_i . Since a clique in a tensor product graph must project to a clique in each of its factors, the maximal order of a clique in the product graph cannot exceed the maximal order in any of the factor graphs, hence is the minimum of the maxima. \square

We now take a definition from Section 2 of [9].

Definition 2.3. The **distant-set** of a point is the set of points distant to it, and its **neighbourhood** is the complement of its distant-set.

We find listed in [9], among the properties of projective spaces of small rings, the cardinalities of the intersections of the neighbourhoods of n mutually distant points, a number there denoted by $\cap nN$. There is a general formula for this quantity (with the same notation as in Proposition 2.2).

Proposition 2.4. $\cap nN = |J| \sum_{k=0}^n (-1)^k \binom{n}{k} \prod_i (q_i + 1 - k)$

Proof. The intersection of a set of complements is the complement of their union, and the cardinality of the union can be calculated by inclusion-exclusion. A set of k mutually distant points is a k -clique and so the number of points in the intersection of all their distant-sets is just the number of $k + 1$ -cliques containing that k -clique, viz. $|J| \prod_i (q_i + 1 - k)$. Given n mutually distant points, there are $\binom{n}{k}$ k -fold intersections among their distant sets, and each k -fold intersection has $|J| \prod_i (q_i + 1 - k)$ points, so by inclusion-exclusion, their union contains

$$- |J| \sum_{k=1}^n (-1)^k \binom{n}{k} \prod_i (q_i + 1 - k)$$

points. The total number of points in the projective line, viz. $|J| \prod_i (q_i + 1)$, is just the value of the expression inside the sum for $k = 0$, so, taking the complement of the union, we have:

$$\cap nN = |J| \sum_{k=0}^n (-1)^k \binom{n}{k} \prod_i (q_i + 1 - k)$$

\square

There is not much to be said about this sum, except for the quirky combinatorial fact, which we prove in Appendix A, that $p | \cap nN$ for every prime $p \leq n$. Hence $\cap 5N$ is always a multiple of 30, and so forth.

3 Counting formulas for general finite rings

We now turn to the non-commutative case. Some results for small non-commutative rings are briefly tabulated in [10].

Let R be a finite ring and let J be its Jacobson radical. We will make use of a definition and some theorems from [3].

Definition 3.1. Two points p and q of a projective line are **radically parallel**, $p||q$, just if they have the same distant sets.

This is not the same as the definition in [3], but by their Corollary 2.3 it is equivalent.

Proposition 3.2. *The points of the form $R(1, a)$ for $a \in J$ form an equivalence class under the relation of radical parallelism.*

Proof. This follows immediately from [3] Theorem 2.1. □

Proposition 3.3. *Two points of the form $R(1, a)$ for $a \in J$ are not mutually distant.*

Proof. We can not possibly have $\begin{pmatrix} 1 & a \\ 1 & b \end{pmatrix} \in \text{GL}_2(R)$ with $a, b \in J$, since it sends (r, s) to $(r + s, ra + sb)$, and the second element of the latter pair will always lie in the Jacobson radical. □

Since the distant graph is vertex transitive, every vertex lies in such a set of order $|J|$ of mutually non-distant points sharing their distant-sets. Since the points of such a set are mutually non-distant, taking the quotient of the graph by the identification of radically parallel points gives a perfectly good surjective morphism of graphs. We might hope that this quotient is the distant graph of the projective line of the quotient of R by J , and Theorem 2.2 of [3], with the immediately preceding discussion, shows just this.

Proposition 3.4. $\mathbb{P}(R/J) \cong \mathbb{P}(R) / ||$.

This extremely convenient result means that, in the finite (or, generally, Artinian) case, we can easily deal with projective lines over rings with non-trivial Jacobson radical by reducing to the quotient, and only need to worry about semisimple rings, which, by the Artin-Wedderburn theorem, means direct sums of matrix rings over finite fields (in the finite case). As we already know how to deal with direct sums, our remaining task is to characterise, so far as possible, the projective lines over matrix rings over finite fields.

Let us start by counting the points of $\mathbb{P}(M_m(q))$, the projective line over the ring of $m \times m$ matrices over the field \mathbb{F}_q of order q .

Proposition 3.5. $|\mathbb{P}(M_m(q))|$ is the q -binomial coefficient $\begin{bmatrix} 2m \\ m \end{bmatrix}_q = \prod_{k=0}^{m-1} \frac{q^{2m-k} - 1}{q^{k+1} - 1}$.

Proof. We shall prove this by assigning an admissible pair to each point. First we observe, from inspecting the form of the multiplication, that $M_2(M_m(q))$ is a lightly disguised version of $M_{2m}(q)$, and likewise $\text{GL}_2(M_m(q))$ is $\text{GL}_{2m}(q)$. Each admissible pair forms the top row of an element of $\text{GL}_2(M_m(q))$, but we can treat these top rows equivalently as the top m rows of an element of $M_{2m}(q)$, i.e. as an $m \times 2m$ matrix in its own right. That these m rows actually belong to an invertible $2m \times 2m$ matrix amounts to the requirement that they span an m -dimensional space (that is, that there are no linear relations among them).

Now, two admissible pairs are equivalent just if they are related by multiplication on the left by an invertible element of the ring, i.e. by an element of $\text{GL}_m(q)$. The left action of $\text{GL}_m(q)$ interchanges every basis of the given subspace while preserving the subspace itself. Hence we have one point of $\mathbb{P}(M_m(q))$ for each m -dimensional subspace of a $2m$ dimensional space over \mathbb{F}_q . The number of these subspaces is the q -binomial coefficient. □

It is also true, by continuing the argument of the proof to all $2m$ rows of the matrix, that two points are distant just when the corresponding subspaces have trivial intersection. (These facts about matrix rings are mentioned in passing in [1]).

Here are the values for the smallest m , after which the polynomials become more complicated:

m	$\left[\begin{array}{c} 2m \\ m \end{array} \right]_q$
0	1
1	$q + 1$
2	$q^4 + q^3 + 2q^2 + q + 1$
3	$q^9 + q^8 + 2q^7 + 3q^6 + 3q^5 + 3q^4 + 3q^3 + 2q^2 + q + 1$

(Of course, $m = 0$ corresponds to the trivial ring, and $m = 1$ to the field of order q .)

Proposition 3.6. For a matrix ring $M_m(q)$,

a) The number of points distant to a given point is q^{m^2} .

b) The number of points distant to a pair of mutually distant points is $\prod_{k=0}^{m-1} (q^m - q^k)$.

$$c) \cap 1N = \prod_{k=0}^{m-1} \frac{q^{2m-k} - 1}{q^{k+1} - 1} - q^{m^2}$$

$$d) \cap 2N = \prod_{k=0}^{m-1} \frac{q^{2m-k} - 1}{q^{k+1} - 1} - 2q^{m^2} + \prod_{k=0}^{m-1} (q^m - q^k).$$

For a product of matrix rings $\prod_i M_{m_i}(q_i)$

$$e) \cap 1N = \prod_i \prod_{k=0}^{m_i-1} \frac{q_i^{2m_i-k} - 1}{q_i^{k+1} - 1} - \prod_i q_i^{m_i^2}$$

$$f) \cap 2N = \prod_i \prod_{k=0}^{m_i-1} \frac{q_i^{2m_i-k} - 1}{q_i^{k+1} - 1} - 2 \prod_i q_i^{m_i^2} + \prod_i \prod_{k=0}^{m_i-1} (q_i^{m_i} - q_i^k)$$

Proof. (Note that a) and b) follow straightforwardly from results for a general ring R .)

a) As the distant graph is vertex transitive, each vertex has the same degree. Hence we can choose, for example, to count the points distant to $R(1, 0)$. The points distant to this are just $R(r, 1)$ for $r \in R$, so their number is just the order of the ring; for $M_m(q)$, this is q^{m^2} .

b) As the distant graph is also edge transitive, the number of points distant to two mutually distant points is always the same, so we can choose points $R(1, 0)$ and $R(0, 1)$. The points distant to both of these are just those of the form $R(u, 1)$, where u is a unit of R . The units of $M_m(q)$ are just the elements of $GL_m(q)$, and $|GL_m(q)| = \prod_{k=0}^{m-1} (q^m - q^k)$.

c) and d) These follow from inclusion-exclusion on the clique counts, as with the commutative case.

e) and f) Each term is a count of k -cliques, for k successively equal to 1, 2 and (in the second case) 3, which is given by the products of the clique-counts for the summand rings. \square

For small m , this gives us the following table for $M_m(q)$:

m	$\cap 1N$	$\cap 2N$
0	0	0
1	1	0
2	$q^3 + 2q^2 + q + 1$	$q^2 + 2q + 1$
3	$q^8 + 2q^7 + 3q^6 + 3q^5 + 3q^4 + 3q^3 + 2q^2 + q + 1$	$q^7 + 3q^6 + 4q^5 + 4q^4 + 2q^3 + 2q^2 + q + 1$

Remark 3.7. Because the distant-graph over the trivial ring has a self-loop, the formulas for $m = 0$ imply that there is 1 k -clique for every k . In the other cases, with no self-loops, clique-counting works properly.

We can also try to count 4-cliques and hence calculate $\cap 3N$. As $\text{GL}_2(R)$ acts transitively on triangles for any projective line, we can, without loss of generality, take three of the points of the clique to be $(1, 0)$, $(0, 1)$ and $(1, 1)$ and ask how many ways there are to extend this. Points distant to all 3 of these points must be of the form $(u, 1)$ where the u are invertible elements such that $u - 1$ is also invertible; in terms of matrices, this means matrices with no eigenvalues equal to 0 or 1. We can handle this by counting matrices which *do* have such eigenvalues, and excluding them.

For this purpose, we will introduce a lemma on inclusion-exclusion. Consider the following setup: a vector space X of dimension m over \mathbb{F}_q , a set \mathcal{G} , and a relation, *capture*, between elements of \mathcal{G} and subspaces of X , subject to the following conditions:

- a) If $g \in \mathcal{G}$ captures a subspace U , then it also captures all subspaces of U .
- b) The cardinality of the set of elements capturing a given subspace depends only on the dimension of that subspace.

For concreteness, the example we have in mind has \mathcal{G} being the set of endomorphisms of X and “captures U ” being “acts as the identity when restricted to U ”.

Let us write W_U for the set of elements that capture U , and $W_{m,k}$ for the cardinality of the set of elements capturing a subspace of dimension k in a space of dimension m . Now condition a) implies that if $U \subseteq V$ then $W_U \supseteq W_V$. Let us write W'_U for the subset of W_U whose elements do not lie in W_V for any V properly containing U , and $W'_{m,k}$ for the cardinality of W'_U for U of dimension k . Then we have the following.

Lemma 3.8.

$$W'_{m,k} = \sum_{i=0}^{m-k} (-1)^i \begin{bmatrix} m-k \\ i \end{bmatrix}_q q^{\frac{i(i-1)}{2}} W_{m,k+i}$$

Proof. In the q -binomial theorem,

$$\prod_{i=0}^{m-1} (1 + q^i t) = \sum_{i=0}^m t^i q^{\frac{i(i-1)}{2}} \begin{bmatrix} m \\ i \end{bmatrix}_q$$

substitute $t = -1$ to get

$$\sum_{i=0}^m (-1)^i q^{\frac{i(i-1)}{2}} \begin{bmatrix} m \\ i \end{bmatrix}_q = 0$$

Hence

$$\sum_{i=0}^{m-1} (-1)^i q^{\frac{i(i-1)}{2}} \begin{bmatrix} m \\ i \end{bmatrix}_q = -(-1)^m q^{\frac{m(m-1)}{2}}$$

Given a subspace U_k of dimension k in a space of dimension m , let us calculate $W'_{m,k}$ by inclusion-exclusion. By Poincaré duality U_k is contained in $\begin{bmatrix} m-k \\ m-(k+i) \end{bmatrix}_q = \begin{bmatrix} m-k \\ i \end{bmatrix}_q$ subspaces of dimension $k+i$. Also, each of these is captured by $W_{m,k+i}$ elements of \mathcal{G} . Hence if each such subspace appears with a factor of $(-1)^i q^{\frac{i(i-1)}{2}}$ in the inclusion-exclusion, then the lemma will be proved. We show this by induction.

We include U_k itself once. As $(-1)^i q^{\frac{i(i-1)}{2}} = 1$ when $i = 0$, the induction starts correctly.

Now suppose that each $k+j$ -space containing U_k has been included/excluded $(-1)^j q^{\frac{j(j-1)}{2}}$ times for $0 \leq j < i$. Consider an i -space $U_i \supset U_k$. For $0 \leq j < i$, consider the j -spaces U_j with

$U_k \subseteq U_j \subset U_i$. There are $\begin{bmatrix} i \\ j \end{bmatrix}_q$ such subspaces, and each one will have been included $(-1)^j q^{\frac{j(j-1)}{2}}$ times. Hence U_i has already been included/excluded $\sum_{j=0}^{i-1} (-1)^j q^{\frac{j(j-1)}{2}} \begin{bmatrix} i \\ j \end{bmatrix}_q = -(-1)^i q^{\frac{i(i-1)}{2}}$ times. So to cancel this, we need to add it back in $(-1)^i q^{\frac{i(i-1)}{2}}$ times. This completes the induction. \square

Example 3.9. Let \mathcal{G} be the set of all endomorphisms, and let an endomorphism capture a subspace if its restriction to that subspace is the zero endomorphism. In an appropriate basis, an endomorphism capturing a subspace of dimension i is given by a matrix with the first i columns all zero (and no restriction on the other columns), so $W_{m,i} = q^{m(m-i)}$. Then the number of invertible endomorphisms is just $W'_{m,0}$. We have, from Lemma 3.8,

$$\begin{aligned} W'_{m,0} &= \sum_{i=0}^m (-1)^i \begin{bmatrix} m \\ i \end{bmatrix}_q q^{\frac{i(i-1)}{2}} q^{m(m-i)} \\ &= q^{m^2} \sum_{i=0}^m (-q^{-m})^i \begin{bmatrix} m \\ i \end{bmatrix}_q q^{\frac{i(i-1)}{2}} \\ &= q^{m^2} \prod_{i=0}^{m-1} (1 - q^{-m} q^i) \\ &= \prod_{i=0}^{m-1} (q^m - q^i) \end{aligned}$$

where the third step follows from the q -binomial theorem.

Proposition 3.10. *In the distant graph of $\mathbb{P}(M_m(q))$, the number of 4-cliques containing a given 3-clique is*

$$(-1)^m q^{\frac{m(m-1)}{2}} \sum_{i=0}^m \prod_{j=0}^{m-i-1} (1 - q^{m-j})$$

or, equivalently,

$$(-1)^m q^{\frac{m(m-1)}{2}} ((1 - q^m) ((1 - q^{m-1}) \dots ((1 - q^2) ((1 - q) + 1) + 1) \dots + 1) + 1)$$

Proof. From the discussion earlier, the number of 4-cliques containing a given 3-clique is equal to the number of matrices in $M_m(q)$ which have neither 0 nor 1 as an eigenvalue. Let \mathcal{G} be the set of invertible endomorphism of \mathbb{F}_q^m , and let an endomorphism capture a subspace if its restriction to that subspace is the identity. Then the number we seek is $W'_{m,0}$.

Now an element which captures the k -subspace of vectors whose coordinates (in some suitable basis) are all 0 after the k th will have a matrix of the form

$$\left(\begin{array}{c|c} I & * \\ \hline 0 & G \end{array} \right)$$

where I is a $k \times k$ identity matrix, $*$ is anything and G is invertible. Hence $W_{m,k} = q^{k(m-k)} \prod_{i=0}^{m-k-1} (q^{m-k} - q^i)$
Then

$$\begin{aligned}
W'_{m,0} &= \sum_{i=0}^m (-1)^i \begin{bmatrix} m \\ i \end{bmatrix}_q q^{\frac{i(i-1)}{2}} q^{i(m-i)} \prod_{j=0}^{m-i-1} (q^{m-i} - q^j) \\
&= \sum_{i=0}^m (-1)^i \left(\prod_{j=0}^{m-i-1} \frac{q^m - q^j}{q^{m-i} - q^j} \right) q^{\frac{i(i-1)}{2}} q^{i(m-i)} \prod_{j=0}^{m-i-1} (q^{m-i} - q^j) \\
&= \sum_{i=0}^m (-1)^i \left(\prod_{j=0}^{m-i-1} (q^m - q^j) \right) q^{\frac{i(i-1)}{2}} q^{i(m-i)} \\
&= \sum_{i=0}^m (-1)^i \left(\prod_{j=0}^{m-i-1} (q^{m-j} - 1) \right) q^{\frac{(m-i)(m-i-1)}{2}} q^{\frac{i(i-1)}{2}} q^{i(m-i)} \\
&= q^{\frac{m(m-1)}{2}} \sum_{i=0}^m (-1)^i \left(\prod_{j=0}^{m-i-1} (q^{m-j} - 1) \right) \\
&= (-1)^m q^{\frac{m(m-1)}{2}} \sum_{i=0}^m \prod_{j=0}^{m-i-1} (1 - q^{m-j})
\end{aligned}$$

The alternative, nested, form is obtained by gathering terms. \square

For k -cliques with $k > 3$, we cannot produce simple counts in the general case, as we can for commutative rings, because these cliques are no longer all equivalent. For instance, when extending a k -clique to a $k + 1$ -clique, the k -cliques fall into distinct classes distinguished by the number of ways it is possible to extend them. In particular, there are cliques which are inextensible although they do not have the maximal order (for which, see below). We give simple concrete examples of this sort of thing in Appendices B and C.

For a ring R with non-trivial Jacobson radical J , we can calculate $\cap kN$ for R/J , then multiply by $|J|$ to get $\cap kN$ for R , since each vertex of $\mathbb{P}(R)$ is just $|J|$ “copies” of a vertex of $\mathbb{P}(R/J)$.

We can also calculate the maximal order of a clique.

Proposition 3.11. *The maximal order of a clique in $\mathbb{P}(M_m(q))$ is $q^m + 1$.*

Proof. Suppose that the clique contains $(1, 0)$ and $(0, 1)$. (Since the graph is vertex- and edge-transitive, this is no loss of generality.) Then the remaining points of the clique must be of the form $(u, 1)$ for invertible $u \in R$, i.e., in the present context, elements of $\text{GL}_m(q)$. Two elements of this form can belong to the same clique just if $\begin{pmatrix} u_1 & 1 \\ u_2 & 1 \end{pmatrix}$ is invertible, which occurs just when $u_1 - u_2$ is invertible. So let us temporarily confine ourselves to the subgraph whose vertices are members of $\text{GL}_m(q)$ and whose edges lie between matrices whose difference is invertible, and work with cliques in this graph. Note that for any set of matrices $\{u_i\}$ forming a clique, and for any $v \in \text{GL}_m(q)$, the set $\{vu_i\}$ also forms a clique, so all cliques are translates of ones containing the identity matrix.

Now consider, say, the top rows of all the u_i in a clique. These must all be different from one another, lest $u_i - u_j$ not be invertible for some i, j . That leaves a maximum of q^m possibilities, but we must exclude the case of all zeroes. This gives an upper bound of $q^m - 1$ to the size of the maximal clique. To see that this bound is attained, consider any matrix u whose characteristic polynomial is irreducible over \mathbb{F}_q . Then its eigenvalues are all distinct, and each of them is a generator of the group of units $\mathbb{F}_{q^m}^*$, of order $q^m - 1$. So we have, for every eigenvalue λ , $\lambda^i \neq 1$ for $0 < i < q^m - 1$. Now let $u_i = u^i$ for $0 \leq i < q^m - 1$. Suppose $i > j$. Then $u^i - u^j = u^j (u^{i-j} - 1)$, and, by the foregoing, u^{i-j} can have no eigenvalues equal to 1 for $i \neq j$, and hence this difference is invertible. So $\{u_i\}$ is a clique of order $q^m - 1$. (It is, however, not hard to exhibit maximal cliques containing 1 that are not of this form.)

So much for cliques inside $\text{GL}_m(q)$. In $\mathbb{P}(\text{M}_m(q))$, we include all points of the form $(u_i, 1)$ together with $(1, 0)$ and $(0, 1)$. Hence the order of a maximal clique is $q^m + 1$. \square

By the same argument as in the commutative case, the maximal order of a clique in a general finite ring R with Jacobson radical J is the minimum value of $q_i^{m_i} + 1$ across the matrix-ring summands of R/J .

Remark 3.12. The number of elements in an m -dimensional subspace, excluding the 0 vector, is $q^m - 1$. As the subspaces corresponding to distant points intersect only in the 0 vector, a $(q^m + 1)$ -clique contains $q^{2m} - 1$ elements, so, putting back the 0 vector, we get the whole space. Hence the maximal clique corresponds to a spread, and the above theorem is equivalent to a (rather specialised) case of general theorems on the existence of spreads (e.g. [4], Lemma 2).

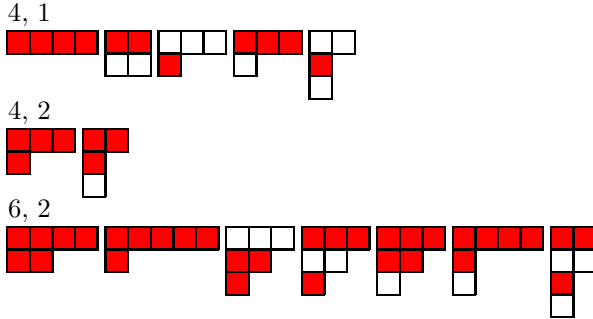
4 Coefficients of clique-extension counts

In this section we shall prove a curious theorem on the coefficients of the higher-order terms for k -clique-extension counts up to $k = 3$. We first introduce some definitions and lemmas (there does not appear to be standard snappy terminology for the concepts defined below).

Definition 4.1. Given some set P_n of partitions of a number n , we say that the **parity-count** of P_n , denoted $\text{PC}(P_n)$, is the number of partitions in P_n with an even number of parts minus the number of partitions in P_n with an odd number of parts.

Definition 4.2. A **distinct partition** is a partition into numbers no two of which are equal. A **2-distinct partition** is a partition whose elements are split across two (possibly empty) subsets, such that each subset consists of distinct elements. An **(h, k, \star) -distinct partition** is a 2-distinct partition of h such that the first subset contains exactly k elements, while the second subset can contain any number of elements. We denote the set of (h, k, \star) -distinct partitions by $\mathcal{D}_2(h, k, \star)$.

To be clear, with (h, k, \star) -distinct partitions we have partitions whose Young diagrams have h boxes divided into (say) red rows and white rows, such that no two red rows have equal length, no two white rows have equal length, and there are exactly k red rows. For example, here are three $\mathcal{D}_2(h, k, \star)$, with $(h, k) = (4, 1)$, $(4, 2)$ and $(6, 2)$.



We may observe that there are just as many partitions in the third row as in the first two together, and this follows from a general lemma.

Lemma 4.3. *There is a bijection $f : \mathcal{D}_2(h, k, \star) \rightarrow \mathcal{D}_2(h - k, k, \star) \cup \mathcal{D}_2(h - k, k - 1, \star)$ such that if $f(x) \in \mathcal{D}_2(h - k, k, \star)$ then x and $f(x)$ have the same number of rows, while if $f(x) \in \mathcal{D}_2(h - k, k - 1, \star)$ then $f(x)$ has one row less than x .*

Proof. From $x \in \mathcal{D}_2(h, k, \star)$, remove one cell from each of the k red rows, giving a 2-distinct partition of $h - k$. If there is a (necessarily unique) red row of length 1 in x , then that row disappears and $f(x) \in \mathcal{D}_2(h - k, k - 1, \star)$, and has one row less than x . If all red rows are longer than 1, then

$f(x) \in \mathcal{D}_2(h-k, k, \star)$ and has the same number of rows as x . This easily reversed operation is clearly a bijection. \square

From the above, it follows not only that the count of partitions in $\mathcal{D}_2(h, k, \star)$ is the sum of the counts in $\mathcal{D}_2(h-k, k, \star)$ and $\mathcal{D}_2(h-k, k-1, \star)$, but also that the parity count of $\mathcal{D}_2(h, k, \star)$ is the difference of the parity counts: $\text{PC}(\mathcal{D}_2(h, k, \star)) = \text{PC}(\mathcal{D}_2(h-k, k, \star)) - \text{PC}(\mathcal{D}_2(h-k, k-1, \star))$, since subtracting one row from every partition in a set simply changes the sign of the parity count. (We do not exclude the empty partition from our counts.)

Definition 4.4. An **m -bounded partition** is a partition whose largest element is no larger than m , and which contains no more than m elements. (That is, one whose Young diagram fits into an $m \times m$ grid.)

Lemma 4.5. *The coefficient of q^{m^2-h} in $(-1)^m q^{\frac{m(m-1)}{2}} \prod_{j=0}^{m-1} (1 - q^{m-j})$ is the parity-count of the m -bounded distinct partitions of h .*

Proof. This is clear from inspecting the way that each term is built when expanding the product. \square

We now have a generalisation of the above lemma.

Lemma 4.6. *Let $h \leq m$. Then the coefficient of q^{m^2-h} in $(-1)^m q^{\frac{m(m-1)}{2}} \prod_{j=0}^{m-1-k} (1 - q^{m-j})$ is equal to the parity-count of $\mathcal{D}_2(h, k, \star)$.*

Proof. Let $P_k(q) = \sum_{i=0}^{m^2} a_i^{(k)} q^i$, for some k with $0 \leq k \leq m$ have the following property (P):

$$a_{m^2-h}^{(k)} = \text{PC}(\mathcal{D}_2(h, k, \star)) \text{ for } h \leq C + \frac{k(k+1)}{2} \quad (\text{P})$$

for some constant C . That is, $P_k(q)$ is a sort of partial generating function for these parity counts. We have, from the remarks following Lemma 4.3, that

$$\text{PC}(\mathcal{D}_2(h, k, \star)) = \text{PC}(\mathcal{D}_2(h-k, k, \star)) - \text{PC}(\mathcal{D}_2(h-k, k-1, \star))$$

and hence

$$\text{PC}(\mathcal{D}_2(h-k, k-1, \star)) = \text{PC}(\mathcal{D}_2(h-k, k, \star)) - \text{PC}(\mathcal{D}_2(h, k, \star))$$

Now suppose that $P_k(q)$ has property (P) and let $P_{k-1}(q) = P_k(q)(1 - q^k)$. This implies $a_{m^2-(h-k)}^{(k-1)} = a_{m^2-(h-k)}^{(k)} - a_{m^2-h}^{(k)}$ for $h \leq C + \frac{k(k+1)}{2}$, i.e. for $h-k \leq C + \frac{(k-1)k}{2}$. By the above recurrence, therefore, $P_{k-1}(q)$ also has property (P) with the same constant C . Now let $P_m(q) = (-1)^m q^{\frac{m(m-1)}{2}}$. This has property (P) for at least $C = 0$, as the number of (h, m, \star) -partitions is 0 for $h < \frac{m(m+1)}{2}$ and 1 for $h = \frac{m(m+1)}{2}$, and hence $\text{PC}(\mathcal{D}_2(h, m, \star)) = 0$ for $h < \frac{m(m+1)}{2}$ and $\text{PC}(\mathcal{D}_2(h, m, \star)) = (-1)^m$ for $h = \frac{m(m+1)}{2}$. Hence we know that property (P) holds with $C = 0$ for all $P_k(q)$ down to $k = 0$. However, we also know from Lemma 4.5 that for $k = 0$, property (P) holds with $C = m$. We know that for $k = 1$, property (P) holds with $C = 0$; that is, we know the coefficients for $h = 0, 1$. Then we can use the recurrence relation $a_{m^2-(h-k)}^{(k-1)} = a_{m^2-(h-k)}^{(k)} - a_{m^2-h}^{(k)}$ with $k = 1$ to extend this to lower-order coefficients until we run out of known coefficients in $P_0(q)$ at $h-k = m$, i.e. $h = m+1$. So property (P) holds with $C = m$ for $k = 1$ also. We now repeat this with $P_2(q)$. We know the coefficients for $h \leq 3$, so we can use the recurrence to extend to lower orders (by jumps of k , i.e. 2) until we run out of known coefficients in $P_1(q)$, at $h-k = m+1$, i.e. $h = m+1+2$. So property (P) holds with $C = m$ for $k = 2$ also. In this way we can continue extending until $k = m$, at each stage

calculating enough coefficients to make property (P) hold with $C = m$. This is more than enough to establish the lemma. \square

Proposition 4.7. *Let $C_{m,k}(q)$ be the (polynomial giving the) number of ways to extend a k -clique to a $k + 1$ -clique in $\mathbb{P}(M_m(q))$. Let $k \leq 3$ and $h \leq m$. Then the coefficient of q^{m^2-h} in $C_{m,k}(q)$ is equal to the coefficient of q^h in $\prod_{i=1}^{\infty} (1 - q^i)^{k-1}$.*

Proof. For $k = 0$, $C_{m,k}(q) = \begin{bmatrix} 2m \\ m \end{bmatrix}_q$. But the coefficient of q^h in this is well-known to be the number of m -bounded partitions of h , and, as the q -binomial coefficient is symmetrical under $k \rightarrow m - k$, this is the same as the coefficient of q^{m^2-h} . Also, $\prod_{i=1}^{\infty} (1 - q^i)^{-1}$ is well-known to be the generating function of the number of partitions, as is clear by expanding this expression, which coincides with the number of m -bounded partitions when $h \leq m$.

For $k = 1$, $C_{m,k}(q) = q^{m^2}$ and $\prod_{i=1}^{\infty} (1 - q^i)^0 = 1$.

For $k = 2$, $C_{m,k}(q) = (-1)^m q^{\frac{m(m-1)}{2}} \prod_{j=0}^{m-1} (1 - q^{m-j})$, and as we have already established, the coefficient of q^{m^2-h} in here is $\text{PC}(\mathcal{D}_2(h, k, \star))$ if $h \leq m$. By essentially the same reasoning, this coincides with the coefficient of q^h in $\prod_{i=1}^{\infty} (1 - q^i)^1$.

For $k = 3$, $C_{m,k}(q) = (-1)^m q^{\frac{m(m-1)}{2}} \sum_{i=0}^m \prod_{j=0}^{m-i-1} (1 - q^{m-j})$. By Lemma 4.6, this is the sum of $\text{PC}(\mathcal{D}_2(h, k, \star))$ for all $h \leq m$, hence equal to the parity-count of all 2-distinct partitions of h such that both subsets are m -bounded. For $h \leq m$, the m -bounding is automatic, and it is not hard to see that $\prod_{i=1}^{\infty} (1 - q^i)^2$ is the generating function for parity-counts of all 2-distinct partitions. \square

Remark 4.8. The coefficients of $\prod_{i=1}^{\infty} (1 - q^i)^{k-1}$ for $k = 0, 1, 2, 3$ are given by OEIS sequences A000041, A000007, A010815 and A002107 ([11]).

Corollary 1. *The leading term of $\cap kN$ for $\mathbb{P}(M_m(q))$ is of degree $m^2 - k$ for $1 \leq k \leq 3$ and has coefficient 1.*

Proof.

$$\cap kN = \sum_{i=0}^k (-1)^i \binom{k}{i} C_{m,k}(q)$$

For sufficiently large m , the leading coefficients of $C_{m,k}(q)$ correspond to the first few coefficients of $\prod_{i=1}^{\infty} (1 - q^i)^{k-1}$, so the leading coefficients of $\cap kN$ correspond to the first few coefficients of $\sum_{j=0}^k (-1)^j \binom{k}{j} \prod_{i=1}^{\infty} (1 - q^i)^{j-1} = \prod_{i=1}^{\infty} (1 - q^i)^{-1} (1 - \prod_{i=1}^{\infty} (1 - q^i))^k$. Since the lowest-degree non-zero term of $1 - \prod_{i=1}^{\infty} (1 - q^i)$ is q , the lowest degree of its powers successively increases by 1, and hence the degree of the leading term of $C_{m,k}(q)$ decreases with k in the same manner.

More explicitly, the coefficients of $C_{m,k}(q)$ start off like this:

	m^2	$m^2 - 1$	$m^2 - 2$	$m^2 - 3$	$m^2 - 4$
$C_{m,0}$	1	1	2	3	5
$C_{m,1}$	1	0	0	0	0
$C_{m,2}$	1	-1	-1	0	0
$C_{m,3}$	1	-2	-1	2	1

Hence the coefficients of $\cap kN$ start off like this:

	m^2	$m^2 - 1$	$m^2 - 2$	$m^2 - 3$	$m^2 - 4$
$\cap 1N$	0	1	2	3	5
$\cap 2N$	0	0	1	3	5
$\cap 3N$	0	0	0	1	4

It only remains to check the cases where $m < k$. We have already done this for $k = 1$ and $k = 2$ in the previous section. It is also easy to check for $k = 3$. Indeed, $C_{0,3} = 1$, $C_{1,3} = q - 2$ and $C_{2,3} = q^4 - 2q^3 - q^2 + 3q$, so where the coefficients are present, they have the needed values. \square

The proof of Proposition 4.7 gives the impression that the theorem really consists of four unrelated facts, one for each value of k . It seems unlikely that this impression is accurate. Here is a sketch of how this pattern arises, showing how the $k = 1$ case should imply the $k = 2$ case, and the $k = 2$ case should imply the $k = 3$ case. In fact, the same mechanism should apply to any clique consisting of $(1, 0)$ together with elements of the form $(\lambda I, 1)$ for $\lambda \in \mathbb{F}_q$.

A function such that, for $h \leq m$, its coefficient for the term of order q^{m^2-h} is the same as the coefficient of q^h in $\prod_{i=1}^{\infty} (1 - q^i)^{k-1}$ is $q^{m^2} \prod_{i=1}^{\infty} (1 - q^{-i})^{k-1}$. Suppose $C_{m,k}$ is sufficiently approximated by this form. Now suppose we are moving up to $k + 1$, and suppose we are choosing among matrices that are candidates for extending a $k - 1$ -clique to a k -clique, but are not necessarily candidates for extending to a $k + 1$ -clique—on account of capturing a non-trivial subspace. Then let us suppose that a matrix that captures the subspace where all coordinates after the i th are 0 is of the form

$$\left(\begin{array}{c|c} A & * \\ \hline B & G \end{array} \right)$$

where A and B are fixed, of sizes $i \times i$ and $(m - i) \times i$ respectively, $*$ can be anything, of size $i \times (m - i)$, and G is one of the $C_{m-i,k}$ matrices of size $(m - i) \times (m - i)$ that would be candidates for a clique-extension in a space of dimension $m - i$. Now, by hypothesis, $C_{m-i,k}$ is approximated by $q^{(m-i)^2} \prod_{j=0}^{\infty} (1 - q^{-j})^{k-1}$, while the number of possible submatrices $*$ is $q^{i(m-i)}$, so from Lemma 3.8, the count of extensions is (approximately)

$$\begin{aligned} & \sum_{i=0}^m (-1)^i \begin{bmatrix} m \\ k \end{bmatrix}_q q^{\frac{i(i-1)}{2}} q^{i(m-i)} q^{(m-i)^2} \prod_{j=1}^{\infty} (1 - q^{-j})^{k-1} \\ &= \sum_{i=0}^m (-1)^i \begin{bmatrix} m \\ k \end{bmatrix}_q q^{\frac{i(i-1)}{2}} q^{m^2} q^{-mi} \prod_{j=1}^{\infty} (1 - q^{-j})^{k-1} \\ &= q^{m^2} \sum_{i=0}^m (-q^{-m})^i \begin{bmatrix} m \\ k \end{bmatrix}_q q^{\frac{i(i-1)}{2}} \prod_{j=1}^{\infty} (1 - q^{-j})^{k-1} \\ &= q^{m^2} \prod_{i=0}^{m-1} (1 - q^{-m} q^i) \prod_{j=1}^{\infty} (1 - q^{-j})^{k-1} \\ &= q^{m^2} \prod_{i=1}^m (1 - q^{-i}) \prod_{j=1}^{\infty} (1 - q^{-j})^{k-1} \end{aligned}$$

(where the third step comes from the q -binomial theorem).

However,

$$\begin{aligned}
& q^{m^2} \prod_{i=1}^m (1 - q^{-i}) \prod_{j=1}^{\infty} (1 - q^{-j})^{k-1} \\
& \approx q^{m^2} \prod_{i=1}^{\infty} (1 - q^{-i}) \prod_{j=1}^{\infty} (1 - q^{-j})^{k-1} \\
& = \prod_{j=1}^{\infty} (1 - q^{-j})^k
\end{aligned}$$

Acknowledgements

I would like to thank John Baez for many helpful comments that improved this paper in several ways.

References

- [1] A. Blunck, Regular spreads and chain geometries, *Bull. Belg. Math. Soc. Simon Stevin* **6,4** (1999), 589–603.
- [2] A. Blunck and H. Havlicek, Projective representations I: Projective lines over rings, *Abh. Math. Sem. Univ. Hamburg* **70** (2000), 287–299.
- [3] A. Blunck and H. Havlicek, Radical parallelism on projective lines and non-linear models of affine spaces, *sl Mathematica Pannonica* **14** (2003), 113–127.
- [4] T. Bu, Partitions of a vector space, *Discrete Mathematics* **31** (1980), 79–83.
- [5] A. Deitmar, Schemes over \mathbb{F}_1 , in *Number Fields and Function Fields—Two Parallel Worlds*, Progr. Math. **239**, Birkhäuser Boston, Boston MA, 2005, 87–100
- [6] J. Han, The general linear group over a ring, *Bull. Korean Math. Soc.* **43** (2006) 619–626.
- [7] A. Herzer, Chain Geometries, in *Handbook of Incidence Geometry*, Elsevier, Amsterdam, 1995, pp. 781–842.
- [8] R. Raghavendran, Finite associative rings, *Comp. Mathematica* **21** (1969) 195–229.
- [9] M. Saniga, M. Planat, M. R. Kibler, P. Pracna, A classification of the projective lines over small rings, *Chaos, Solitons and Fractals* **33,4** (2007) 1095–1102.
- [10] M. Saniga, M. Planat, M. R. Kibler, P. Pracna, A classification of the projective lines over small rings II. Non-commutative case. Available from [⟨arXiv:math/0606500⟩](https://arxiv.org/abs/math/0606500).
- [11] N. J. A. Sloane, editor, The On-Line Encyclopedia of Integer Sequences. Available at <https://oeis.org>

A A combinatorial identity

Here we prove the remark that we have $p | \cap n\mathbb{N}$ for every prime $p \leq n$, where

$$\cap n\mathbb{N} = |J| \sum_{k=0}^n (-1)^k \binom{n}{k} \prod_i (q_i + 1 - k)$$

Observe that the sum is of the form $\sum_k (-1)^k \binom{n}{k} f(k)$, where $f(k)$ is a function whose value mod p depends only on $k \bmod p$ for every p , so that the sum separates into terms of the form $\sum_j (-1)^{jp+m} \binom{n}{jp+m} f(m)$ (where j ranges over all values such that $0 \leq jp+m \leq n$). But we have the following theorem.

Proposition A.1.
$$\sum_{\substack{j \\ 0 \leq jp+m \leq n}} (-1)^{jp+m} \binom{n}{jp+m} = 0 \pmod{p} \text{ for prime } p \leq n$$

Proof. Let ϕ be a primitive p th root of unity.

$$\begin{aligned} & \frac{1}{p} \sum_{j=0}^{p-1} (1 - \phi^j)^n \phi^{-jm} \\ &= \frac{1}{p} \sum_{j=0}^{p-1} \sum_{k=0}^n (-1)^k \binom{n}{k} \phi^{jk} \phi^{-jm} \\ &= \sum_{k=0}^n (-1)^k \binom{n}{k} \left\{ \frac{1}{p} \sum_{j=0}^{p-1} \phi^{j(k-m)} \right\} \end{aligned}$$

The term in braces is 0 unless $(k-m)$ is a multiple of p , in which case it is 1, so the whole expression is equal to the alternating lacunary sum above.

But on the other hand, if $p \leq n$, then every term in the first sum contains a factor of the form

$$(1 - \phi^j)^p$$

But, mod p , this is equal to $1 - \phi^{jp} = 0$. □

B Inequivalent cliques

Here is an example of why we can not expect to have a general formula for the number of ways to extend a k -clique for $k > 3$. Suppose $m = 2$ and $q = 3$. Let us work in $\text{GL}_2(3)$, where (to abuse the definition a little) we will say that two elements are distant if their difference is invertible. Suppose we have already picked the following 3-clique:

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix} \right\}$$

There are 9 elements which will extend this to a 4-clique, and they fall into 3 classes:

$$\mathbf{A} = \left\{ \begin{pmatrix} 2 & 2 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \right\}$$

$$\mathbf{B} = \left\{ \begin{pmatrix} 2 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix} \right\}$$

$$\mathbf{C} = \left\{ \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix} \right\}$$

All the elements of \mathbf{A} are mutually distant, all the elements of \mathbf{B} are mutually distant, and the single element of \mathbf{C} is distant to everything in \mathbf{A} and \mathbf{B} ; but no element of \mathbf{A} is distant to any element of \mathbf{B} . This means that at this point, we are committed to forming one of two maximal

cliques (with 8 elements), *viz.* by appending either $\mathbf{A} \cup \mathbf{C}$ or $\mathbf{B} \cup \mathbf{C}$ to our existing 3-clique. Now, if we form a 4-clique by appending the single element of \mathbf{C} , the resulting clique can be extended to a 5-clique in 8 ways (by appending any element of \mathbf{A} or \mathbf{B}). However, if instead we choose an element of \mathbf{A} , the resulting 4-clique will only be extensible to a 5-clique in 4 ways (by appending either the element of \mathbf{C} or another element of \mathbf{A}), and similarly for \mathbf{B} . So there are (at least) two kinds of 4-clique, with different extension counts.

If we extend by $\mathbf{A} \cup \mathbf{C}$, then we get a maximal clique not generated as powers of a single matrix.

C Inextensible submaximal clique

Here is a clique in $\text{GL}_2(\mathbb{F}_5)$ that is inextensible but has only 20 elements.

$$\begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 0 & 2 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 0 & 3 \\ 3 & 1 \end{pmatrix} \begin{pmatrix} 0 & 4 \\ 4 & 2 \end{pmatrix} \\ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 2 & 0 \end{pmatrix} \begin{pmatrix} 1 & 3 \\ 3 & 0 \end{pmatrix} \\ \begin{pmatrix} 1 & 4 \\ 4 & 3 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 2 \\ 2 & 3 \end{pmatrix} \\ \begin{pmatrix} 2 & 3 \\ 3 & 3 \end{pmatrix} \begin{pmatrix} 2 & 4 \\ 4 & 0 \end{pmatrix} \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} 3 & 1 \\ 1 & 1 \end{pmatrix} \\ \begin{pmatrix} 3 & 2 \\ 2 & 2 \end{pmatrix} \begin{pmatrix} 3 & 3 \\ 3 & 2 \end{pmatrix} \begin{pmatrix} 3 & 4 \\ 4 & 1 \end{pmatrix} \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}$$

D The limit $q \rightarrow 1$

Theorems and formulas that hold generally over finite fields \mathbb{F}_q also often have a true combinatorial interpretation in the case $q = 1$. This is the case with our counting formulas.

We can define (e.g. Section 5.1 of [5]) the general linear group $\text{GL}_n(\mathbb{F}_1)$ over the fictitious one-element field to consist of $n \times n$ permutation matrices—those with a single entry of 1 in each row and each column, all other entries being 0. These matrices act by permuting rows (from the left) or columns (from the right) and $\text{GL}_n(\mathbb{F}_1)$ is isomorphic to the symmetric group S_n . We can go on to define $\text{GL}_n(\mathbb{F}_{1^n})$ over “extensions of the one-element field”, which are the same as elements of $\text{GL}_n(\mathbb{F}_1)$ except that instead of entries being 1, they may be any n th root of unity; this group is isomorphic to the wreath product of S_n and the cyclic group Z_n .

A point in $\mathbb{P}(\text{M}_m(\mathbb{F}_1))$ consists of the first m rows of a $2m \times 2m$ permutation matrix, modulo multiplication from the left by $m \times m$ permutation matrices. Since the latter permute rows arbitrarily, we only care which columns contain a 1, not which row they appear in, so the number of points is $\binom{2m}{m}$, i.e. the $q \rightarrow 1$ limit of $\left[\begin{matrix} 2m \\ m \end{matrix} \right]_q$. Given a choice for the filled columns of the first m rows, there is only one choice for the remaining m rows, *viz.* the remaining unfilled places, so only one point is distant to a given point. This is the $q \rightarrow 1$ limit of q^{m^2} , as we would hope. There are then of course no extensions to cliques of 3 or 4 points, and this is again given by the $q \rightarrow 1$ limits of the clique extension polynomials, which equal 0. Moving to extensions of \mathbb{F}_1 results in no change: multiplication from the left by elements of $\text{GL}_m(\mathbb{F}_{1^n})$ allows us not only to arbitrarily permute rows but also to reduce all non-zero entries to 1.

Hence the distant graph of $\text{M}_m(\mathbb{F}_{1^n})$ consists of $\binom{2m}{m}$ points, arranged into mutually distant pairs.