Subgraphs of the projective norm graph*

Tomas Bayer† Tamás Mészáros‡ Lajos Rónyai§ Tibor Szabó¶

May 23, 2021

Abstract

The limited dependence between the additive and the multiplicative structure of fields is in the background of a number of explicit constructions of various types of pseudorandom objects. In this direction we study the size of the intersection of (the additive) translates of fibers of the (multiplicative) norm function over finite fields. Besides extending earlier upper bounds, our main focus here is on obtaining lower bounds.

From our results we conclude several consequences in extremal combinatorics. Our motivation is the projective norm graph $\mathrm{NG}(q,t)$ and its small subgraph statistics. $\mathrm{NG}(q,t)$ provides a tight construction for the Turán number of complete bipartite graphs $K_{t,s}$ with $s > (t-1)!$, in particular it does not contain $K_{t,(t-1)!+1}$. Yet, for $t \geq 4$ it is not even known whether $\mathrm{NG}(q,t)$ contains $K_{t,t}$. The determination of the largest integer $s(t)$, such that $\mathrm{NG}(q,t)$ contains $K_{t,s(t)}$ for all large enough prime powers q is an important open question with far-reaching consequences and the best known bounds, $t-1 \leq s(t) \leq (t-1)!$, are very far apart. In this paper we settle the first open case and establish $s(4) = 6$. Along the way we also count subgraphs of $\mathrm{NG}(q,t)$ isomorphic to H, for any fixed 3-degenerate graph H, and find that projective norm graphs are quasirandom with respect to these parameters. These results go beyond the consequences of the Expander Mixing Lemma and also imply extensions of the work of Alon and Shikhelman on generalized Turán numbers.

Finally, we also give an elementary proof of the $K_{4,s}$-freeness of $\mathrm{NG}(q,t)$ for $s = 6(\sum_{i=0}^{t-4} q^i) + 1$. This was known before for $t = 4$ only, via a less direct algebro-geometric argument.

Keywords: Turán problem, quasirandomness, norm graphs, finite fields, norm equations
Mathematics Subject Classification (2020): 05C25, 05C35, 11T06

1 Introduction

Among both the earliest and most thoroughly studied problems in extremal graph theory are *Turán*-type problems. Given a graph H and positive integer n, the *Turán number of* H, denoted by $\mathrm{ex}(n,H)$, is the maximum number of edges a simple graph on n vertices may have without containing a subgraph isomorphic to H. The very first result about Turán numbers is Mantel's theorem [48] from 1907, stating that $\mathrm{ex}(n,K_3) = \lfloor \frac{n^2}{4} \rfloor$. In 1941 Turán [71] determined $\mathrm{ex}(n,K_t)$ exactly for every $t \geq 3$ and identified the

*This manuscript is the outcome of combining the results of the arxiv preprints [14] and [49], each of which dealt with a subset of finite fields, together covering all cases. The motivation behind the restructuring is to offer a more conscise treatment, which handles the characteristic independent parts of the arguments uniformly. The automorphism group result from [14] is now separated into a short note [16]. The results of this paper appeared without proof in an extended abstract [15] of the EUROCOMB 2019 conference.

†Email: tomasbayer@gmail.com.

‡Freie Universität Berlin, Institut für Mathematik, Berlin, Germany. Email: tamas.meszaros@fu-berlin.de. Supported by a DRS Fellowship of Freie Universität Berlin.

§Institute for Computer Science and Control, Budapest, Hungary, and Budapest University of Technology and Economics. Email: ronyai.lajos@sztaki.mta.hu.

¶Freie Universität Berlin, Institut für Mathematik, Berlin, Germany. Email: szabo@math.fu-berlin.de. Supported by GIF grant G-1347-304.6/2016.

unique extremal examples. For arbitrary H, a corollary of the Erdős-Stone Theorem [30], formulated by Erdős and Simonovits [29], gives

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

where $\chi(H)$ is the chromatic number of H. If H is not bipartite, this theorem determines $\mathrm{ex}(n,H)$ asymptotically.

For bipartite graphs H the Erdős-Stone-Simonovits theorem merely states that $\mathrm{ex}(n,H)$ is of lower than quadratic order. A general classification of the order of magnitude of bipartite Turán numbers is widely open, even in the simplest-looking cases of even cycles and complete bipartite graphs. Among even cycles the order of magnitude of the Turán number is known only for C_4, C_6 and C_{10} [17, 28]. For the Turán number of complete bipartite graphs a general upper bound,

$$\mathrm{ex}(n,K_{t,s})\le\frac{1}{2}\sqrt[t]{s-1}\cdot n^{2-\frac{1}{t}}+\frac{t-1}{2}\cdot n,$$

was proven by Kővári, T. Sós and Turán [41] using an elementary double counting argument. In general it is commonly conjectured (see e.g. [19, 23]) that the order of magnitude in the KST theorem is the right one.

Conjecture 1. *For every $t,s\in\mathbb{N}$, $t\le s$,*

$$\mathrm{ex}(n,K_{t,s})=\Theta\left(n^{2-\frac{1}{t}}\right).$$

To prove a matching lower bound, one needs to exhibit a $K_{t,s}$-free graph that is dense enough. A general lower bound of $\Omega(n^{2-\frac{s+t-2}{st-1}})$ can be obtained using the probabilistic method, but this is of smaller order for all values of the parameters. Constructions with number of edges matching the order of the upper bound were first found for $K_{2,2}$-free graphs (Klein, lásd [28]) and later for $K_{3,3}$-free graphs (Brown [21]). Füredi determined the correct leading coefficient for $K_{2,s}$-free graphs [32] and for $K_{3,3}$-free graphs [33].

Kollár, Rónyai and Szabó [38] proved Conjecture 1 for every $t\ge 4$ and $s>t!$ by constructing for every $t\in\mathbb{N}^+$ a family of graphs, called norm graphs, that are $K_{t,t!+1}$-free and their density matches the order of magnitude of the KST upper bound. Later Alon, Rónyai and Szabó [5] modified this construction to verify the conjecture for $s>(t-1)!$. One way or another all these $K_{t,s}$-free constructions of optimal density are based on the simple geometric intuition that t "average", "generic" hypersurfaces in the t-dimensional space are "expected" to have a 0-dimensional intersection. In manifestations of this idea the neighborhoods of vertices are such hypersurfaces and the common neighborhood of t vertices more or less corresponds to the degree of their intersection. Recently Blagojević, Bukh and Karasev [18] and later Bukh [22] implemented the idea in a random setting, where the neighborhoods are determined by random polynomials. This gave an alternative proof of the tightness of Conjecture 1 for $s=f(t)$, with $f(t)$ much larger than $(t-1)!$.

Despite significant effort by numerous researchers in the last sixty years, the fundamental question about the Turán number of $K_{t,t}$ is wide open, even in the case of $t=4$. For $\mathrm{ex}(n,K_{4,4})$ or even for $\mathrm{ex}(n,K_{4,6})$, it is not even known whether they are of larger order than $n^{\frac{5}{3}}=\Theta(\mathrm{ex}(n,K_{3,3}))$.

1.1 The projective norm graphs

Let $q=p^k$ be a prime power, $t\ge 2$ be an integer and let $\mathrm{N}_t=\mathrm{N}_{t,q}:\mathbb{F}_{q^t}\to\mathbb{F}_q$ denote the $\mathbb{F}_q$-*norm on* $\mathbb{F}_{q^t}$, i.e. $\mathrm{N}_t(A)=A\cdot A^q\cdot A^{q^2}\cdots A^{q^{t-1}}$ for $A\in\mathbb{F}_{q^t}$. Alon et al. [5] defined the *projective norm graph* $\mathrm{NG}(q,t)$ as the graph with vertex set $\mathbb{F}_{q^{t-1}}\times\mathbb{F}_q^*$ and vertices (A,a) and (B,b) being adjacent if $\mathrm{N}_{t-1}(A+B)=ab$. The graph $\mathrm{NG}(q,t)$ has $q^{t-1}\cdot(q-1)=:n$ vertices. To count the edges, one can consider an arbitrary vertex $(A,a)\in\mathbb{F}_{q^{t-1}}\times\mathbb{F}_q^*$ and determine its degree. For this note that for any choice of $X\in\mathbb{F}_{q^{t-1}}\backslash\{-A\}$ there is a unique x, namely $x=\frac{1}{a}\cdot\mathrm{N}_{t-1}(A+X)$, for which (X,x) is a neighbour, unless it is the same vertex as (A,a). This happens exactly if $\mathrm{N}_{t-1}(2A)=a^2$. Vertices satisfying the latter equality will be called *loop vertices*. The degree of a non-loop vertex then is $q^{t-1}-1$, while it is one less for a loop vertex. The number of loop

vertices is $q^{t-1}-1$ if $\mathrm{Char}(\mathbb{F}_q)\neq 2$ and zero if $\mathrm{Char}(\mathbb{F}_q)=2$. Now, the number of edges can be precisely calculated:

$$e(\mathrm{NG}(q,t))=\begin{cases}\frac{1}{2}\left(q^{t-1}-1\right)q^{t-1}(q-1) & \text{if } q \text{ is a power of 2}\\ \frac{1}{2}\left(q^{t-1}-1\right)\left(q^{t-1}(q-1)-1\right) & \text{otherwise.}\end{cases}$$

In other words, the number of edges in both cases is[1] $\approx \frac{1}{2}q^{2t-1}\approx\frac{1}{2}n^{2-\frac{1}{t}}$. Relying largely on a general algebro-geometric lemma from [38], it was shown in [5] that $\mathrm{NG}(q,t)$ is $K_{t,(t-1)!+1}$-free. Since $\mathrm{NG}(q,t)$ also has the desired density, it verifies Conjecture 1 for $s>(t-1)!$.

Since their first appearance, (projective) norm graphs were studied extensively [7, 11, 12, 36, 39, 55, 60]. Their various properties were utilized in many otherareas, both within and outside combinatorics. These include, among others, (hypergraph) Ramsey theory [6, 40, 45, 50, 53, 54, 74, 75], (hypergraph) Turán theory [3, 7, 56, 57, 60, 61], other problems in extremal combinatorics, [2, 13, 47, 62, 66, 67], number theory [58, 64, 72, 73], geometry [31, 59] and computer science [1, 9, 10, 27].

A drawback of the proof of the $K_{t,(t-1)!+1}$-freeness of $\mathrm{NG}(q,t)$ in [5] is that it does not give any information about complete bipartite subgraphs with other parameters. In particular, for $t\geq 4$ it could even be the case that there is an infinite sequence of prime powers q such that $\mathrm{NG}(q,t)$ does not contain $K_{t,t}$ and hence resolves the question of the order of magnitude of $\mathrm{ex}(n,K_{t,s})$ for every t and s. Considering the fundamental nature of Conjecture 1, it was already suggested in [38] that the determination of the largest integer $s(t)$, such that $\mathrm{NG}(q,t)$ contains $K_{t,s(t)}$ for *every* large enough prime power q is a question of great interest, with potentially far reaching consequences. The main result of [5] implies $s(t)\leq(t-1)!$ and by simple combinatorial reasons (the KST upper bound), $\mathrm{NG}(q,t)$ does contain $K_{t,t-1}$, so $s(t)\geq t-1$. For $t=2$ and $t=3$ the upper and lower bound agree, so $s(2)=1$, $s(3)=2$. The bounds for $t\geq 4$ however are very far apart: $t-1\leq s(t)\leq(t-1)!$. If $s(t)$ were found to be less than $(t-1)!$ then the projective norm graphs verified Conjecture 1 for more values of the parameters than what is known currently. In particular, as already mentioned before, for the Turán number of $K_{4,6}$ no better lower bound than $\mathrm{ex}(n,K_{3,3})=\Theta(n^{\frac{5}{3}})$ is known.

There was/is a reasonable amount of hope that the method of [5] was not optimal for $\mathrm{NG}(q,t)$, and that the projective norm graphs might also not contain $K_{t,s}$ for some $s\leq(t-1)!$. This optimism is mainly inspired by the generality of the key lemma of [38] used in the proof. That lemma provides very general conditions, under which the system of equations

$$\prod_{j=1}^{t}(x_j-a_{i,j})=b_i,\quad i\in[t]$$

over any field $\mathbb{F}$ has at most $t!$ solutions $(x_1,\ldots,x_t)\in\mathbb{F}^t$. Namely, it was enough to assume for the constants $a_{i,j},b_i\in\mathbb{F}$, that $a_{i_1,j}\neq a_{i_2,j}$ whenever $i_1\neq i_2$. For the application one has to use the lemma for the field $\mathbb{F}_{q^{t-1}}$ and only in the special case when $a_{i,j}=a_{i,1}^{q^{j-1}}$ for every $i,j\in[t]$. Moreover, one is interested in bounding the number of only those solutions for which $x_j=x_1^{q^{j-1}}$ for every $j\in[t]$. That is, the key lemma is used for a very special choice of constants and very special type of solutions.

In this direction Grosu [36] showed that there is a sequence of primes, of density $\frac{1}{9}$, such that for any prime p in this sequence $\mathrm{NG}(p,4)$ does contain a $K_{4,6}$. This result nevertheless does not even exclude the possibility that $s(4)=3$. About complete bipartite graphs with a larger smaller partite set Ball and Pepe [11, 12] proved that the $K_{t,(t-1)!+1}$-free projective norm graphs do not contain a $K_{t+1,(t-1)!-1}$ either. This in particular improved the earlier probabilistic lower bound on $\mathrm{ex}(n,K_{5,5})$.

2 Our results.

In this paper we show that for arbitrary prime power $q\geq 5$, the projective norm graph $\mathrm{NG}(q,4)$ contains many copies of $K_{4,6}$, hence $s(4)=6$. Our method is different from Grosu's. On the way, we determine

[1] In this paper the asymptotic notation involving the projective norm graph is always understood with q tending to ∞ and t being a constant.

asymptotically the number of copies of any fixed 3-degenerate graph in $\mathrm{NG}(q,4)$. This has implications to the quantitative quasirandom properties of projective norm graphs and extends results of Alon and Shikhelman [7] on generalized Turán numbers. In the process we also uncover a close connection between norm equation systems and the classic Singer difference sets. Furthermore, we also give a new, commutative algebra-free proof of the $K_{4,7}$-freeness of $\mathrm{NG}(q,4)$. This argument extends to estimating the size of the common neighborhoods of four element vertex sets in $\mathrm{NG}(q,t)$, for arbitrary $t \geq 4$. For $t \geq 5$ this is not known to follow from the proof in [5, 38]. We are hopeful that direct arguments like this might shed more light on the structure of projective norm graphs in general.

Next we state our results in detail.

2.1 Norm equation systems

Understanding containment of complete bipartite subgraphs in the projective normgraph boils down to being able to determine the size of the intersection of translates of fibres of the norm function. It is well-known and not difficult to see that the fibres of non-zero elements of $\mathbb{F}_q$ partition the non-zero elements of $\mathbb{F}_{q^t}$ into equal parts. Since translation does not change their size, we have that for every $A \in \mathbb{F}_{q^t}$ and $a \in \mathbb{F}_q^*$, the equation $N_t(X+A)=a$ has exactly $\frac{q^t-1}{q-1}$ solutions $X \in \mathbb{F}_{q^t}$.

It is less clear how many common solutions two or more such norm equations have. For a set $U = \big\{(A_1,a_1),\dots,(A_\ell,a_\ell)\big\} \subseteq \mathbb{F}_{q^t} \times \mathbb{F}_q^*$ of coefficients we are interested in the number of solutions $X \in \mathbb{F}_{q^t}$ of the system of ℓ norm equations

$$\mathrm{N}_t(A_i+X)=a_i, \quad i \in [\ell]. \tag{1}$$

The set of solutions will be denoted by $\mathrm{S}_t(U)$. In [37] it was shown that when the number ℓ of equations is equal to the degree t of the field extension, and the A_i are all distinct, then the number of solutions cannot be more than $t!$. Note that if $A_i = A_j$ for some $i \neq j$ then either there is no solution (if $a_i \neq a_j$) or two equations coincide (if $a_i = a_j$). We call a set $U = \big\{(A_1,a_1),\dots,(A_\ell,a_\ell)\big\} \subseteq \mathbb{F}_{q^t} \times \mathbb{F}_q^*$ of coefficients *generic* if the first coordinates are all distinct.

In our first theorem we determine the size of the intersection of translates of two fibers. For $t=2$ our result is precise, while for $t \geq 3$ it is mostly asymptotic. We are also able to characterize the degenerate cases, when the intersection of the two fibers is *not* around the "average" $(1+o(1))q^{t-2}$. Curiously this can only happen when the degree of the field extension is at most three.

To state our results we introduce some more notation. We denote by $\mathrm{Tr}_t = \mathrm{Tr}_{t,q}$ the $\mathbb{F}_q$-trace function on $\mathbb{F}_{q^t}$, i.e. for $X \in \mathbb{F}_{q^t}$ we have $\mathrm{Tr}_t(X) := X + X^q + \cdots + X^{q^{t-1}}$, and for odd q we let $\eta_{\mathbb{F}_q}$ denote the quadratic character of $\mathbb{F}_q$. Finally, for an integer q, let $res_3(q) \in \{-1,0,1\}$ denotes the residue of q modulo 3.

Theorem 1. *Let $q=p^k$ be a prime power, $t \geq 2$ be an integer, and $U = \big\{(A_1,a_1),(A_2,a_2)\big\} \subseteq \mathbb{F}_{q^t} \times \mathbb{F}_q^*$ be a generic set of coefficients. Further put*

$$c_1 = c_1\big((A_1,a_1),(A_2,a_2)\big) = \frac{a_1}{\mathrm{N}(A_2-A_1)} \in \mathbb{F}_q^* \quad \text{and} \quad c_2 = c_2\big((A_1,a_1),(A_2,a_2)\big) = \frac{a_2}{\mathrm{N}(A_2-A_1)} \in \mathbb{F}_q^*.$$

(a) If $t=2$ then

$$\big|S_2(U)\big| = \begin{cases} 1-\eta_{\mathbb{F}_q}\big((1+c_1-c_2)^2-4c_1\big) & \text{if } q \text{ odd,} \\ 1 & \text{if } p=2 \text{ and } c_1+c_2=1, \\ 1-(-1)^{\mathrm{Tr}_{k,2}\left(\frac{c_1}{(1+c_1+c_2)^2}\right)} & \text{if } p=2 \text{ and } c_1+c_2 \neq 1. \end{cases}$$

(b) If $t \geq 3$ then

$$\big|S_t(U)\big| = \begin{cases} 2q+1-res_3(q) & \text{if } t=3, \text{ and } (c_1,c_2)=(1,-1) \\ q^{t-2}+O(q^{t-2.5}) & \text{otherwise,} \end{cases}$$

Our second main theorem deals with the intersection of translates of three fibres.

Theorem 2. *Let $q = p^k$ be a prime power and $t \geq 3$ be an integer.*

(a) For every generic set $U = \big\{(A_1, a_1), (A_2, a_2), (A_3, a_3)\big\} \subseteq \mathbb{F}_{q^t} \times \mathbb{F}_q^*$ of coefficients, we have

$$\big|S_t\,(U)\,\big| \leq 6\big(q^{t-3} + q^{t-4} + \cdots + q + 1\big).$$

(b) If $q \geq 5$ and $t = 3$ then there exists a generic set $U = \big\{(0,1), (1,-1), (A,-1)\big\} \subseteq \mathbb{F}_{q^3} \times \mathbb{F}_q^*$, such that $A \neq 1$, $N_3(A) = 1$, and

$$\big|S_3\,(U)\,\big| = 6.$$

The upper bound of (a) for $t = 3$ was proved in [37] using a different argument. Part (b) shows that this upper bound is tight.

2.2 Difference sets

The proof of part (b) of Theorem 2 crucially depends on a characterization of the solutions of (1) in the canonical exceptional case from Theorem 1(b). On the one hand, we show that $S_3\big((0,1),(1,-1)\big)$ is the union of the roots of two simple polynomials of degree $q+1$, each of which factors in $\mathbb{F}_{q^3}$. On the other hand, the root set of both polynomials turns out to be a difference set within the multiplicative cyclic group $\mathcal{N} = \{X \in \mathbb{F}_{q^3} : N_3(X) = 1\}$ of order $q^2 + q + 1$.

Given a multiplicative group $\mathcal{G}$, a subset $\mathcal{D} \subseteq \mathcal{G}$ is called a *planar difference set* if every non-identity element $A \in \mathcal{G}$ has a unique representation as a product of an element from $\mathcal{D}$ and an element from $\mathcal{D}^{-1}$, where $\mathcal{D}^{-1} := \{d^{-1} : d \in \mathcal{D}\}$ denotes the set of inverses of the elements of $\mathcal{D}$. We refer to this representation as the *mixed representation of A with respect to $\mathcal{D}$*. If the group $\mathcal{G}$ admits a planar difference set of size m, then, by simple counting, its order has to be of the form $\ell^2 + \ell + 1$ with $\ell = m + 1$. Planar difference sets in Abelian groups are only known to exist if the group is cyclic and ℓ is a prime power. As it will cause no confusion, in what follows we will omit the word 'planar'. For a gentle introduction and a good survey on difference sets the reader may consult e.g. [51].

Theorem 3. *Let $q \geq 2$ be a prime power. Then we have*

$$S_3\Big(\big\{(0,1),(1,-1)\big\}\Big) = \mathcal{H}_1 \cup \mathcal{H}_2,$$

where

$$\mathcal{H}_1 = \big\{X \in \overline{\mathbb{F}}_q : X^{q+1} + X + 1 = 0\big\} \qquad \text{and} \qquad \mathcal{H}_2 = \big\{X \in \overline{\mathbb{F}}_q : X^{q+1} + X^q + 1 = 0\big\},$$

where $\overline{\mathbb{F}}_q$ denotes the algebraic closure of $\mathbb{F}_q$. The sets $\mathcal{H}_1, \mathcal{H}_2$ form difference sets in the multiplicative group $\mathcal{N} \subseteq \mathbb{F}_{q^3}$, and $\mathcal{H}_2 = \mathcal{H}_1^{-1}$. Furthermore for any element $A \in \mathcal{N} \setminus \{1\}$, its unique mixed representation $A = A_1 \cdot A_2$ is given by the following explicit formulas:

$$A_1 = \frac{A^{q+1} - 1}{1 - A^q} \in \mathcal{H}_1 \qquad \text{and} \qquad A_2 = \frac{A - A^{q+1}}{A^{q+1} - 1} \in \mathcal{H}_2. \tag{2}$$

The difference sets $\mathcal{H}_1$ and $\mathcal{H}_2$ turn out to be of the classic Singer type[2]. Their simple description from the theorem, as roots of two sparse polynomials, seems novel, at least we did not find it in the literature. In any case, the difference set property and the explicit expression of mixed representations will be crucial in the proof of our main result.

[2]We discuss Singer difference sets in a more general setting in Section 5.3 of the Appendix.

2.3 Common neighborhoods

Our results about norm equation systems transfer in a relatively standard way to common neighborhoods of small vertex sets in the projective norm graphs. For a set $T = \big\{(V_i, v_i) \in \mathbb{F}_{q^{t-1}} \times \mathbb{F}_q^* : \ i \in [\ell]\big\}$ of ℓ vertices of $\mathrm{NG}(q,t)$, we define the *common neighbourhood* of T as the set

$$\Gamma(T) = \big\{(Y,y) \in V\big(\mathrm{NG}(q,t)\big) : \mathrm{N}_{t-1}(Y+V_i) = yv_i, \ i \in [\ell]\big\} \subseteq \mathbb{F}_{q^{t-1}} \times \mathbb{F}_q^*.$$

Note that in our definition we do allow a vertex to be in its own neighborhood. The size of $\Gamma(T)$ is the *common degree* of T and is denoted by $\deg(T)$. With this notation the main result of Alon, Rónyai and Szabó [5] can be phrased as $\deg(T) \le (t-1)!$ for every subset $T \subseteq V\big(\mathrm{NG}(q,t)\big)$ of size t.

A moment of thought reveals that two vertices of the projective norm graph with the same first coordinate do not have a common neighbour in $\mathrm{NG}(q,t)$. In particular, the common neighborhood of a non-generic set of vertices is empty. The following proposition formulates how exactly the common neighbors of a generic set of ℓ vertices are related to solutions of a system of $\ell - 1$ norm equations of type (1).

Proposition 1. *Let $T = \big\{(V_i, v_i) : i \in [\ell]\big\} \subseteq V\big(\mathrm{NG}(q,t)\big)$ be an arbitrary generic set. Then the set $A(T) := \big\{(A_i(T), a_i(T)) : i \in [\ell-1]\big\}$, defined through*

$$A_i(T) := \frac{1}{V_i - V_\ell} \in \mathbb{F}_{q^{t-1}}^* \qquad \text{and} \qquad a_i(T) := \frac{v_i}{v_\ell \cdot \mathrm{N}_{t-1}(V_i - V_\ell)} \in \mathbb{F}_q^*,$$

is also generic, and the function Φ that maps (Y,y) to $\frac{1}{Y+V_\ell}$, is a bijection from $\Gamma(T)$ to $S_{t-1}\big(A(T)\big) \setminus \{0\}$.[3] *In particular, we have*

$$\deg(T) = \Big|S_{t-1}\big(A(T)\big)\Big| - \xi(T),$$

where

$$\xi(T) = \begin{cases} 1 & \text{if } v_1 = \cdots = v_\ell \\ 0 & \text{otherwise.} \end{cases}$$

For a pair $T = \big\{(V_1, v_1), (V_2, v_2)\big\}$ of vertices, Proposition 1 implies that the common degree of T is either $\frac{q^{t-1}-1}{q-1}$ (if $v_1 \neq v_2$) or one less (if $v_1 = v_2$).

The results of Theorem 1 and Theorem 2(a) translate via Proposition 1 to results on the common degrees of triples and quadruples of vertices of $\mathrm{NG}(q,t)$, respectively.

In the particular case $t = 3 = \ell$ the proof of Füredi [33] strengthening the Kővári-Sós-Turán upper bound, coupled with the fact that $\mathrm{NG}(q,3)$ is $K_{3,3}$-free, implies that roughly half of the triples in $\mathrm{NG}(q,3)$ must have two common neighbors and roughly half of them have none. Theorem 1(a) and Proposition 1 together characterize triples of each type; we skip the explicit statement.

Next we spell out the direct consequences of Theorem 1(b) and Theorem 2(a), which will also be necessary for our subsequent applications on quasirandomness and generalized Turán numbers.

Corollary 1. *Let $q = p^k$ be a prime power, $t \ge \ell$ be integers, and $T = \big\{(V_i, v_i) : i \in [\ell]\big\}$ be a generic ℓ-subset of vertices in $\mathrm{NG}(q,t)$.*

(a) If $\ell \in \{2,3\}$ and $t > \ell$, then $\deg(T) = q^{t-\ell} + O\left(q^{t-\ell-\frac{1}{2}}\right)$, unless $\ell = 3$, $t = 4$, $\frac{v_1}{v_3}\,\mathrm{N}\left(\frac{V_2-V_3}{V_1-V_2}\right) = 1$ and $\frac{v_2}{v_3}\,\mathrm{N}\left(\frac{V_1-V_3}{V_1-V_2}\right) = -1$, in which case $\deg(T) = 2q + O(1)$.

(b) If $\ell = 4$, then $\deg(T) \le 6\left(q^{t-4} + q^{t-3} + \cdots + q + 1\right)$.

Part (b) is an extension of the result of [5] on the $K_{4,7}$-freeness of $\mathrm{NG}(q,4)$, and its proof uses more elementary tools than the one based on [38].

Finally, from Theorem 2(b) and Proposition 1 we infer that the $K_{4,7}$-free projective norm graph $\mathrm{NG}(q,4)$ contains (many) $K_{4,6}$ for every prime power larger than 4.

[3] For the sake of the precise definition of the set $A(T)$ and the function Φ, we fix an arbitrary ordering of the elements of $\mathbb{F}_{q^{t-1}}$ and we take V_ℓ to be, say, the minimal among $\{V_i, i \in [\ell]\}$.

Corollary 2. *For every prime power $q = p^k \geq 5$ there are at least $\Omega\left(q^{10}\right)$ copies of $K_{4,6}$ in the (simple) projective norm graph* $\mathrm{NG}(q,4)$. *In particular,* $s(4) = 6$.

Complementing Corollary 2 we remark that it is immediate that $\mathrm{NG}(2,4)$ does not contain $K_{4,6}$, and in $\mathrm{NG}(3,4)$ and $\mathrm{NG}(4,4)$ we verified by computer search that there is no $K_{4,6}$ either.

2.4 Quasirandomness

A (sequence of) graph(s) G on n vertices with average degree $d = d(n)$ is called *quasirandom* if it possesses some property that the Erdős-Rényi binomial random graph $G\left(n, \frac{d(n)}{n}\right)$ also has with probability tending to 1 as n tends to infinity. For dense graphs G, i.e. when $\frac{d}{n}$ is constant, many of these natural properties are known to be equivalent. (see the seminal papers of Thomason [69, 70], and Chung, Graham, and Wilson [25]). These include properties

Q1 for any two large enough subsets A, B of vertices, the number of edges going between them is $\approx \frac{d}{n}\big|A\big|\big|B\big|$;

Q2 for most pairs of vertices their common degree is $\approx \frac{d^2}{n}$;

Q3 for any fixed graph H, the number of labeled copies of H is $\approx n^{v(H)}\left(\frac{d}{n}\right)^{e(H)}$;

Q4 $\lambda(G)$, the second largest among the absolute values of eigenvalues of G, is of smaller order than the degree d (which is the largest eigenvalue).

For sparse graphs, i.e., when $d = o(n)$, the relationship between these properties was investigated in several papers [24, 26, 37]. Properties **Q1** and **Q2**, for example, always follow from **Q4** by the Expander Mixing Lemma [8], with a smaller second eigenvalue implying stronger quasirandomness. Some of the implications however, in contrast to the dense case, are far from being true. It is an interesting general problem to quantify the extent to which one of these properties implies another.

The projective norm graphs, in particular, serve as examples for some of the equivalences being false. Alon and Rödl [6] and Szabó [68] showed that the eigenvalues of $\mathrm{NG}(q,t)$ are exactly ± 1 times the absolute values of the different Gaussian sums over the field $\mathbb{F}_{q^{t-1}}$, and hence, the second largest absolute value of an eigenvalue is $\lambda = \lambda\big(\mathrm{NG}(q,t)\big) = q^{\frac{t-1}{2}}$. That is, not only λ is of smaller order than the degree $d \approx q^{t-1}$, so **Q4** holds, but λ is roughly the square root of the degree. As it is well-known (and not hard to see, e.g., [42]) that for every d-regular graph on n vertices $\lambda = \Omega\big(\sqrt{d}\big)$ (provided the density $\frac{d}{n}$ is bounded away from 1), the projective norm graphs are *as quasirandom as it gets*, at least in terms of their second eigenvalue. Still, **Q3** can fail for an arbitrary large inverse polynomial density $n^{-\alpha}$, $\alpha > 0$. For example, $\mathrm{NG}(q,4)$ does not contain any $K_{4,7}$, but the random graph $G\big(n, n^{-\frac{1}{4}}\big)$ contains many, namely $\Theta\big(n^4\big)$ copies.

Even though **Q3** might fail for certain graphs, it is an interesting problem to quantify to what extent the "perfect quasirandomness" of $\mathrm{NG}(q,t)$ in terms of property **Q4** carries over to property **Q3**. To this end we will call a graph G *H-quasirandom* if property **Q3** holds for H, that is, if the number $X_H(G)$ of labeled copies of H in G is $\Theta\left(n^{v(H)}\left(\frac{d}{n}\right)^{e(H)}\right)$. If $X_H(G) = \big(1+o(1)\big)n^{v(H)}\left(\frac{d}{n}\right)^{e(H)}$, then we say that G is *asymptotically H-quasirandom*. With this notion any regular graph is asymptotically K_2-quasirandom and the projective norm graph $\mathrm{NG}(q,t)$ is not $K_{t,(t-1)!+1}$-quasirandom.

Alon and Pudlák [4] (see also [42]) have shown, using the Expander Mixing Lemma, that any d-regular graph G on n vertices with second eigenvalue λ (such graphs are also called (n,d,λ)-*graphs*) and $\lambda \ll \frac{d^\Delta}{n^{\Delta-1}}$ contains $\big(1+o(1)\big)n^{v(H)}\left(\frac{d}{n}\right)^{e(H)}$ labeled copies of any H with maximum degree at most Δ. In our terminology they have shown that an (n,d,λ)-graph with small enough λ is asymptotically H-quasirandom.

For the projective norm graph this means that if $\Delta(H) < \frac{t+1}{2}$, then $\mathrm{NG}(q,t)$ is H-quasirandom. For $\Delta = 2$ this statement starts to work when t is at least 4 and for $\Delta = 3$ it starts to work when t is at least 6. Using Corollary 1 we can go *beyond* what is possible in terms of subgraph containment from the general

eigenvalue bound of the Expander Mixing Lemma, and can deal with the much wider class of degenerate graphs instead of just bounded maximum degree. Recall that a graph G is r-degenerate if every nonempty subgraph of G has a vertex of degree at most r, or equivalently, there is an ordering of the vertices of G such that every vertex has at most r neighbours preceding it.

Theorem 4. *Let $q = p^k$ be a prime power and H a simple graph. Then, for the number of vertex labeled copies of H in $\mathrm{NG}(q,t)$, we have*

$$X_H\big(\mathrm{NG}(q,t)\big) = \Theta\left(q^{tv(H)-e(H)}\right), \tag{3}$$

as q tends to infinity, provided H is 3-degenerate and $t \geq 4$. That is, $\mathrm{NG}(q,t)$ is H-quasirandom. Moreover, if H is 3-degenerate and $t \geq 5$ or H is 2-degenerate and $t \geq 3$, then

$$\left|X_H\big(\mathrm{NG}(q,t)\big) - q^{t\cdot v(H)-e(H)}\right| \leq O\left(q^{tv(H)-e(H)-\frac{1}{2}}\right). \tag{4}$$

In particular, $\mathrm{NG}(q,t)$ is asymptotically H-quasirandom in these cases.

Remarks. As $\mathrm{NG}(q,3)$ does not contain $K_{3,3}$ and $\mathrm{NG}(q,2)$ does not contain $K_{2,2}$, the bound on t for (3) is best possible for both 3- and 2-degenerate graphs. We conjecture though that the stronger statement (4) should also be true for 3-degenerate graphs and $t = 4$. Also, the theorem remains valid even if $H = H_q$ and $v = v(H_q)$ grows moderately, namely if $v(H_q) = o(\sqrt{q})$ as q tends to infinity, with an error term $o\big(q^{tv(H)-e(H)}\big)$ in (4).

2.5 Generalized Turán numbers

For simple graphs T and H (with no isolated vertices) and a positive integer n, the generalized Turán problem asks for the maximum possible number $\mathrm{ex}(n,T,H)$ of unlabeled copies of T in an H-free graph on n vertices. Note that by setting $T = K_2$ we recover the original Turán problem for H. Alon and Shikhelman [7] investigated the problem in the case when H is a complete bipartite graph $K_{t,s}$ with $t \leq s$, and T is a complete graph K_ℓ or a complete bipartite graph $K_{a,b}$. They have shown that $K_{t,s}$-freeness in an n vertex graph implies that the number of copies of T is at most $O\left(n^{v(T)-\frac{e(T)}{t}}\right)$, whenever T is a clique K_m with $m \leq t+1$ or a complete bipartite graph $K_{a,b}$ with $a \leq b < s$ and $a \leq t$. This, together with the Alon-Pudlák counting of subgraphs in the projective norm graph implied that for every $s > (t-1)!$, the generalized Turán number

$$ex(n,T,K_{t,s}) = \Theta\left(n^{v(T)-\frac{e(T)}{t}}\right), \tag{5}$$

whenever T is a clique K_m with $m \leq \frac{t+2}{2}$ or a complete bipartite graph $K_{a,b}$ with $a \leq b \leq \frac{t}{2}$. For $T = K_3$, Kostochka, Mubayi and Verstraëte [39] and Alon and Shikhelman [7] counted triangles in the projective norm graphs more directly, which extended (5) from $t \geq 4$ to all $t \geq 2$.

The lower bounds of Theorem 4 extend the eigenvalue lower bound of Alon and Pudlák on generalized Turán numbers for arbitrary 3-degenerate graphs.

Corollary 3. *For every 3-degenerate simple graph T and any $t \geq 4$ and $s > (t-1)!$ we have*

$$\mathrm{ex}(n,T,K_{t,s}) \geq (1+o(1))\frac{1}{|\mathrm{Aut}(T)|}n^{v(T)-\frac{e(T)}{t}}.$$

Combining this result with the upper bound of Alon and Shikhelman [7], we extend the validity of (5) for $T = K_4$ (from $t \geq 6$ to $t \geq 4$) and complete bipartite graphs $K_{3,b}$ (from $t \geq 6$ and $b \leq t/2$ to the best possible $t \geq 4$ and $b < s$).

Corollary 4. *For every $t \geq 4$ and $s > (t-1)!$ we have*

$$ex(n,T,K_{t,s}) = \Theta\left(n^{v(T)-\frac{e(T)}{t}}\right),$$

whenever T is a clique K_4 or a complete bipartite graph $K_{a,b}$ with $a \leq b < s$ and $a \leq 3$.

3 Proofs

3.1 Proof of Theorem 1

To prove Theorem 1 we first transform our system of interest to a simpler form.

Lemma 1. $\left|S_t\big(U\big)\right| = \left|S_t\big(U'\big)\right|$, *where* $U' = \big\{(0,c_1),(1,c_2)\big\}$ *with* c_1, c_2 *as in Theorem 1.*

Proof. For every $Y \in \mathbb{F}_{q^t}$ define $\Psi(Y) = \dfrac{Y + A_1}{A_2 - A_1}$. Then it is a straightforward calculation to show that $Y \in \mathrm{S}_t\big((A_1,a_1),(A_2,a_2)\big)$ if and only if $\Psi(Y) \in \mathrm{S}_t\big((0,c_1),(1,c_2)\big)$, and so the Lemma follows. □

To simplify notation, from now on we will write $\mathrm{S}_t(c_1,c_2)$ instead of $\mathrm{S}_t\big(U'\big) = \mathrm{S}_t\Big(\big\{(0,c_1),(1,c_2)\big\}\Big)$. For $(c_1,c_2) \in (\mathbb{F}_q^*)^2$ and $t \geq 2$ let

$$f_{t,c_1,c_2}(X) = N_{t-1}(X+1)\cdot \mathrm{N}_{t-1}(X) + c_1 \cdot \mathrm{N}_{t-1}(X+1) - c_2 \cdot \mathrm{N}_{t-1}(X) \in \mathbb{F}_q[X].$$

As we will demonstrate shortly, this polynomial is strongly related to our system of norm equations. Let us denote by $\mathrm{R}_t(c_1,c_2)$ the set of roots of f_{t,c_1,c_2} in the algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$, and by $\mathrm{R}_t^*(c_1,c_2) \subseteq \mathrm{R}_t(c_1,c_2)$ the set of multiple roots among them. In the following lemma we connect $\mathrm{S}_t(c_1,c_2)$ to the roots in $\mathrm{R}_t(c_1,c_2)$. It turns out that every root of f_{t,c_1,c_2} is contained in the union of the fields $\mathbb{F}_{q^t}$ and $\mathbb{F}_{q^{t-1}}$. Furthermore all multiple roots are contained in the intersection $\mathbb{F}_{q^t} \cap \mathbb{F}_{q^{t-1}} = \mathbb{F}_q$ and have multiplicity two.

Lemma 2. *For* $(c_1,c_2) \in (\mathbb{F}_q^*)^2$ *and* $t \geq 2$ *we have*

(i) $S_t(c_1,c_2) \subseteq \mathrm{R}_t(c_1,c_2)$;

(ii) $S_t(c_1,c_2) \cap \mathbb{F}_q = \mathrm{R}_t^*(c_1,c_2)$;

(iii) $\big|S_t(c_1,c_2)\big| + \big|\,\mathrm{R}_t(c_1,c_2) \cap \mathbb{F}_{q^{t-1}}\big| = 2\big(q^{t-2} + q^{t-3} + \cdots + 1\big)$.

(iv) For $t \geq 3$

$$\big|S_t(c_1,c_2)\big| = 2\big(q^{t-2} + q^{t-3} + \cdots + 1\big) - \sum_{b \in \mathbb{F}_q^* \setminus \{-c_1\}} \left|S_{t-1}\left(b, \frac{bc_2}{b+c_1}\right)\right|.$$

Proof. First we prove part (i). Let $X \in \mathrm{S}_t(c_1,c_2)$, that is

$$c_1 = \mathrm{N}_t(X) \qquad \text{and} \qquad c_2 = \mathrm{N}_t(X+1).$$

Multiplying the equations by $\mathrm{N}_{t-1}(X+1)$ and $\mathrm{N}_{t-1}(X)$, respectively, and subtracting them from one another we obtain

$$c_1\,\mathrm{N}_{t-1}(X+1) - c_2\,\mathrm{N}_{t-1}(X) = \mathrm{N}_t(X)\,\mathrm{N}_{t-1}(X+1) - \mathrm{N}_t(X+1)\,\mathrm{N}_{t-1}(X).$$

By substituting $\mathrm{N}_t(X) = \mathrm{N}_{t-1}(X)X^{q^{t-1}}$ and $\mathrm{N}_t(X+1) = \mathrm{N}_{t-1}(X+1)(X+1)^{q^{t-1}}$ we get

$$\begin{aligned} c_1\,\mathrm{N}_{t-1}(X+1) - c_2\,\mathrm{N}_{t-1}(X) &= \mathrm{N}_{t-1}(X)\,\mathrm{N}_{t-1}(X+1)X^{q^{t-1}} - \mathrm{N}_{t-1}(X+1)\,\mathrm{N}_{t-1}(X)(X+1)^{q^{t-1}} \\ &= \mathrm{N}_{t-1}(X+1)\,\mathrm{N}_{t-1}(X)\left(X^{q^{t-1}} - (X+1)^{q^{t-1}}\right) = \mathrm{N}_{t-1}(X+1)\,\mathrm{N}_{t-1}(X)(-1). \end{aligned}$$

This proves that X is a root of f_{t,c_1,c_2}, i.e. $X \in \mathrm{R}_t(c_1,c_2)$.

For part (ii) let us first consider an arbitrary $X \in \mathrm{S}_t(c_1,c_2) \cap \mathbb{F}_q$. By part (i) we know that X is a root of f_{t,c_1,c_2}. To show that it is a multiple root, we check that X is also root of the formal derivative f'_{t,c_1,c_2}. As $X \notin \{0,-1\}$, the formal derivative f'_{t,c_1,c_2} at X can be expressed as $\big(q^{t-2} + \cdots + q + 1\big)$ times

$$\left(\frac{\mathrm{N}_{t-1}(X+1)\,\mathrm{N}_{t-1}(X)}{X} + \frac{\mathrm{N}_{t-1}(X+1)\,\mathrm{N}_{t-1}(X)}{X+1} + \frac{c_1\,\mathrm{N}_{t-1}(X+1)}{X+1} - \frac{c_2\,\mathrm{N}_{t-1}(X)}{X}\right).$$

Since $X \in \mathrm{S}_t(c_1, c_2)$, we may again replace c_1 and c_2 by $\mathrm{N}_t(X) = \mathrm{N}_{t-1}(X)X^{q^{t-1}}$ and $\mathrm{N}_t(X+1) = \mathrm{N}_{t-1}(X+1)(X+1)^{q^{t-1}}$, respectively. As $q^{t-2} + \cdots + q + 1 = 1$ in $\mathbb{F}_q$, this results in

$$f'_{t,c_1,c_2}(X) = \mathrm{N}_{t-1}(X)\,\mathrm{N}_{t-1}(X+1)\left(\frac{1}{X} + \frac{1}{X+1} + \frac{X^{q^{t-1}}}{X+1} - \frac{(X+1)^{q^{t-1}}}{X}\right).$$

However, as $X \in \mathbb{F}_q$, we have $X^q = X$, so the last factor simplifies to

$$\frac{1}{X} + \frac{1}{X+1} + \frac{X}{X+1} - \frac{X+1}{X} = 0,$$

proving that $f'_{t,c_1,c_2}(X) = 0$. Consequently $X \in \mathrm{R}^*_t(c_1, c_2)$, hence

$$\mathrm{S}_t(c_1, c_2) \cap \mathbb{F}_q \subseteq \mathrm{R}^*_t(c_1, c_2). \tag{6}$$

Before proving that in (6) we have actually equality, we show part (iii).

We start by bounding the union and intersection of the sets $\mathrm{S}_t(c_1, c_2)$ and $\mathrm{R}_t(c_1, c_2) \cap \mathbb{F}_{q^{t-1}}$. By part (i) we have

$$\mathrm{S}_t(c_1, c_2) \cup \big(\mathrm{R}_t(c_1, c_2) \cap \mathbb{F}_{q^{t-1}}\big) \subseteq \mathrm{S}_t(c_1, c_2) \cup \mathrm{R}_t(c_1, c_2) = \mathrm{R}_t(c_1, c_2).$$

Since $\mathrm{S}_t(c_1, c_2) \subseteq \mathbb{F}_{q^t}$ and $\mathbb{F}_{q^t} \cap \mathbb{F}_{q^{t-1}} = \mathbb{F}_q$, by (i) and (6) we obtain

$$\mathrm{S}_t(c_1, c_2) \cap \mathrm{R}_t(c_1, c_2) \cap \mathbb{F}_{q^{t-1}} = \mathrm{S}_t(c_1, c_2) \cap \mathbb{F}_{q^{t-1}} = \mathrm{S}_t(c_1, c_2) \cap \mathbb{F}_q \subseteq \mathrm{R}^*_t(c_1, c_2).$$

These two observations together imply

$$\big|\mathrm{S}_t(c_1, c_2)\big| + \big|\,\mathrm{R}_t(c_1, c_2) \cap \mathbb{F}_{q^{t-1}}\big| \leq \big|\,\mathrm{R}_t(c_1, c_2)\big| + \big|\,\mathrm{R}^*_t(c_1, c_2)\big|.$$

Now note that as $\big|\,\mathrm{R}_t(c_1, c_2)\big|$ is the number of different linear factors of f_{t,c_1,c_2} in $\overline{\mathbb{F}}_q$ and $\big|\,\mathrm{R}^*_t(c_1, c_2)\big|$ is the number of different linear factors that appear at least twice, their sum is necessarily bounded from above by the degree of f_{t,c_1,c_2} i.e. by $2\big(q^{t-2} + \cdots + q + 1\big)$. This shows

$$\big|\mathrm{S}_t(c_1, c_2)\big| + \big|\,\mathrm{R}_t(c_1, c_2) \cap \mathbb{F}_{q^{t-1}}\big| \leq 2\big(q^{t-2} + \cdots + 1\big). \tag{7}$$

To get the desired equality for every pair $(c_1, c_2) \in (\mathbb{F}^*_q)^2$ we will use a Stepanovesque trick of considering their average and using double counting to transfer the difficult task of bounding the number of solutions of a high degree equation into the easy task of bounding the number of solutions of a linear equation. In other words we will show that the desired equality holds for the average, i.e.,

$$\frac{1}{(q-1)^2} \sum_{c_1 \in \mathbb{F}^*_q} \sum_{c_2 \in \mathbb{F}^*_q} \Big(\big|\mathrm{S}_t(c_1, c_2)\big| + \big|\,\mathrm{R}_t(c_1, c_2) \cap \mathbb{F}_{q^{t-1}}\big|\Big) = 2(q^{t-2} + \cdots + 1). \tag{8}$$

Note that this indeed will be enough, as we have already obtained the same upper bound for the individual terms, so equality for the average is possible only if each individual term matches the upper bound.

To prove (8), we split the sum and evaluate each part separately. For the first part we use double-counting to obtain

$$\sum_{c_1 \in \mathbb{F}^*_q} \sum_{c_2 \in \mathbb{F}^*_q} \big|\mathrm{S}_t(c_1, c_2)\big| = \sum_{X \in \mathbb{F}_{q^t}} \Big|\big\{(c_1, c_2) \in (\mathbb{F}^*_q)^2 \mid \mathrm{S}_t(c_1, c_2) \ni X\big\}\Big| \qquad = \sum_{X \in \mathbb{F}_{q^t} \setminus \{0,-1\}} 1 = q^t - 2.$$

The next to last equality holds since the sets $\mathrm{S}_t(c_1, c_2)$ partition $\mathbb{F}_{q^t} \setminus \{0, -1\}$. Indeed, each $X \in \mathbb{F}_{q^t} \setminus \{0, -1\}$ is contained in exactly one of them, namely $\mathrm{S}_t\big(\mathrm{N}_t(X), \mathrm{N}_t(X+1)\big)$. Similarly,

$$\sum_{c_1 \in \mathbb{F}^*_q} \sum_{c_2 \in \mathbb{F}^*_q} \big|\,\mathrm{R}_t(c_1, c_2) \cap \mathbb{F}_{q^{t-1}}\big| = \sum_{X \in \mathbb{F}_{q^{t-1}}} \sum_{c_1 \in \mathbb{F}^*_q} \Big|\big\{c_2 \in \mathbb{F}^*_q \mid X \in \mathrm{R}_t(c_1, c_2)\big\}\Big|.$$

Now for fixed $X \in \mathbb{F}_{q^{t-1}}$ and $c_1 \in \mathbb{F}_q^*$ the expression $f_{t,c_1,c_2}(X)$ becomes a linear polynomial in c_2. It has no root in $\mathbb{F}_q^*$ if $X \in \{0,-1\}$ or $c_1 = -\mathrm{N}_{t-1}(X)$, otherwise there is a unique c_2 for which $f_{t,c_1,c_2}(X) = 0$, namely $c_2 = \frac{\mathrm{N}_{t-1}(X+1)\left(\mathrm{N}_{t-1}(X)+c_1\right)}{\mathrm{N}_{t-1}(X)}$. Hence

$$\sum_{c_1 \in \mathbb{F}_q^*} \sum_{c_2 \in \mathbb{F}_q^*} \left|\mathrm{R}_t(c_1,c_2) \cap \mathbb{F}_{q^{t-1}}\right| = \sum_{X \in \mathbb{F}_{q^{t-2}} \setminus \{0,-1\}} \; \sum_{c_1 \in \mathbb{F}_q^* \setminus \{-\mathrm{N}_{t-1,q}(X)\}} 1 = (q^{t-1}-2)(q-2).$$

Summing up both parts, we get

$$\sum_{c_1 \in \mathbb{F}_q^*} \sum_{c_2 \in \mathbb{F}_q^*} \left(\left|\mathrm{S}_t(c_1,c_2)\right| + \left|\mathrm{R}_t(c_1,c_2) \cap \mathbb{F}_{q^{t-1}}\right|\right) = q^t - 2 + \left(q^{t-1}-2\right)(q-2) = 2(q-1)^2\left(q^{t-2}+\cdots+1\right),$$

which proves (8).

Now we turn back to finish the proof of (ii). The equality in (iii) implies that in the proof of (7) all displayed inequalities and containments must hold with equality, in particular, we have equality in (6) as well.

Finally, we prove (iv). To express $\left|\mathrm{S}_t(c_1,c_2)\right|$ we first count the elements of $\mathrm{R}_t(c_1,c_2) \cap \mathbb{F}_{q^{t-1}}$ through classifying them by their norm and then use part (iii).

$$\begin{aligned}\left|\mathrm{R}_t(c_1,c_2) \cap \mathbb{F}_{q^{t-1}}\right| &= \sum_{b \in \mathbb{F}_q} \left|\left\{X \in \mathrm{R}_t(c_1,c_2) \cap \mathbb{F}_{q^{t-1}} : \mathrm{N}_{t-1}(X) = b\right\}\right| \\ &= \sum_{b \in \mathbb{F}_q} \left|\left\{X \in \mathbb{F}_{q^{t-1}} : \mathrm{N}_{t-1}(X) = b \text{ and } \mathrm{N}_{t-1}(X+1)(b+c_1) = b \cdot c_2\right\}\right|.\end{aligned}$$

Note that $0 \notin \mathrm{R}_t(c_1,c_2) \cap \mathbb{F}_{q^{t-1}}$, since $c_1 \neq 0$. Hence, for $b = 0$ this set is empty. Moreover, it is also empty for $b = -c_1$, since neither c_1, nor c_2 is 0. Consequently,

$$\begin{aligned}\left|\mathrm{R}_t(c_1,c_2) \cap \mathbb{F}_{q^{t-2}}\right| &= \sum_{b \in \mathbb{F}_q^* \setminus \{-c_1\}} \left|\left\{X \in \mathbb{F}_{q^{t-1}} \mid \mathrm{N}_{t-1}(X) = b \text{ and } \mathrm{N}_{t-1}(X+1) = \frac{b \cdot c_2}{b+c_1}\right\}\right| \\ &= \sum_{b \in \mathbb{F}_q^* \setminus \{-c_1\}} \left|\mathrm{S}_{t-1}\left(b, \frac{b \cdot c_2}{b+c_1}\right)\right|\end{aligned}$$

Now, the assertion of part (iv) follows by part (iii). □

We are now ready to prove Theorem 1. By Lemma 1 it is enough to consider the sets $\mathrm{S}_t(c_1,c_2)$ for $(c_1,c_2) \in (\mathbb{F}_q^*)^2$. We start by examining the case $t = 2$. By part (iii) of Lemma 2 we have

$$\begin{aligned}\left|\mathrm{S}_2(c_1,c_2)\right| &= 2 - \left|\mathrm{R}_2(c_1,c_2) \cap \mathbb{F}_q\right| = 2 - \left|\left\{X \in \mathbb{F}_q \mid f_{2,c_1,c_2}(X) = 0\right\}\right| \\ &= 2 - \left|\left\{X \in \mathbb{F}_q \mid (X+1)X + c_1 \cdot (X+1) - c_2 X = 0\right\}\right| \\ &= 2 - \left|\left\{X \in \mathbb{F}_q \mid X^2 + (1+c_1-c_2)X + c_1 = 0\right\}\right|\end{aligned}$$

If q is odd, then part (i) of Proposition 7 from the Appendix gives

$$\left|\mathrm{S}_2(c_1,c_2)\right| = 2 - \left(1 + \eta_{\mathbb{F}_q}\left((1+c_1-c_2)^2 - 4c_1\right)\right) = 1 - \eta_{\mathbb{F}_q}\left((1+c_1-c_2)^2 - 4c_1\right),$$

while for $q = 2^k$, using part (ii) of Proposition 7 from the Appendix, we get

$$\left|\mathrm{S}_2(c_1,c_2)\right| = \begin{cases} 1 & \text{if } c_1 + c_2 = 1 \\ 2 - \left(1 + (-1)^{\mathrm{Tr}_{k,2}\left(\frac{c_1}{(1+c_1+c_2)^2}\right)}\right) = 1 - (-1)^{\mathrm{Tr}_{k,2}\left(\frac{c_1}{(1+c_1+c_2)^2}\right)} & \text{if } c_1 + c_2 \neq 1 \end{cases}.$$

This finishes the proof of part (a). In the case $t = 3$, by applying part (iv) of Lemma 2 and the case $t = 2$, we obtain

$$\big|\mathrm{S}_3(c_1,c_2)\big| = 2(q+1) - \sum_{b\in\mathbb{F}_q^*\setminus\{-c_1\}} \left|\mathrm{S}_2\left(b, \frac{bc_2}{b+c_1}\right)\right|.$$

Now first suppose again that q is odd. Then

$$\begin{aligned}\big|\mathrm{S}_3(c_1,c_2)\big| &= 2(q+1) - \sum_{b\in\mathbb{F}_q^*\setminus\{-c_1\}} \left(1 - \eta_{\mathbb{F}_q}\left(\left(1+b-\frac{bc_2}{b+c_1}\right)^2 - 4b\right)\right)\\ &= q+4 + \sum_{b\in\mathbb{F}_q^*\setminus\{-c_1\}} \eta_{\mathbb{F}_q}\left(\frac{\big((b+c_1)(1+b)-bc_2\big)^2 - 4b(b+c_1)^2}{(b+c_1)^2}\right).\end{aligned}$$

Put

$$\begin{aligned}L(b) &= \big((b+c_1)(1+b)-bc_2\big)^2 - 4b(b+c_1)^2\\ &= b^4 + 2(c_1-c_2-1)b^3 + \big((1+c_1-c_2)^2 - 6c_1\big)b^2 + 2c_1(1-c_1-c_2)b + c_1^2, \qquad (9)\end{aligned}$$

and observe that the denominator inside $\eta_{\mathbb{F}_q}$ may be omitted as it is a non-zero square and $\eta_{\mathbb{F}_q}$ is multiplicative. Accordingly,

$$\begin{aligned}\big|\mathrm{S}_3(c_1,c_2)\big| &= q+4+\sum_{b\in\mathbb{F}_q^*\setminus\{-c_1\}} \eta_{\mathbb{F}_q}\big(L(b)\big) = q+4-\eta_{\mathbb{F}_q}\big(L(0)\big) - \eta_{\mathbb{F}_q}\big(L(-c_1)\big) + \sum_{b\in\mathbb{F}_q}\eta_{\mathbb{F}_q}\big(L(b)\big)\\ &= q+4-\eta_{\mathbb{F}_q}\left(c_1^2\right) - \eta_{\mathbb{F}_q}\left(c_1^2c_2^2\right) + \sum_{b\in\mathbb{F}_q}\eta_{\mathbb{F}_q}\big(L(b)\big) = q+2+\sum_{b\in\mathbb{F}_q}\eta_{\mathbb{F}_q}\big(L(b)\big).\end{aligned}$$

Our goal is to use the Weil character sum estimate (see Theorem 5 in the Appendix) for the quadratic character $\eta_{\mathbb{F}_q}$. As the order of $\eta_{\mathbb{F}_q}$ is 2, we can estimate the above sum using the first part of Theorem 5, unless $L(b) = (b^2+\alpha_1 b+\alpha_0)^2$ for some $\alpha_1,\alpha_0\in\mathbb{F}_q$, in which case the second part of the theorem applies.

By comparing the coefficients of

$$(b^2+\alpha_1 b+\alpha_0)^2 = b^4 + 2\alpha_1 b^3 + (\alpha_1^2+2\alpha_0)b^2 + 2\alpha_1\alpha_0 b + \alpha_0^2$$

with (9) it is easy to see that the degenerate case occurs if and only if $(c_1,c_2) = (1,-1)$. Indeed, the constant terms imply that $c_1 = \alpha_0$ or $c_1 = -\alpha_0$ and using the coefficients of b and b^3 we have that $2c_1(1-c_1-c_2) = 2\alpha_1\alpha_0 = 2(c_1-c_2-1)\alpha_0$. Substituting $c_1 = -\alpha_0$ leads to $c_2 = 0$, a contradiction. Substituting $c_1 = \alpha_0$ we obtain $\alpha_0 = c_1 = 1$ and $\alpha_1 = -c_2$ and substituting all this into the coefficients of b^2 we obtain $c_2 = -1$.

If $(c_1,c_2) = (1,-1)$, then $L(b) = b^4+2b^3+3b^2+2b+1 = (b^2+b+1)^2$ is indeed a square and we can apply the second part of Theorem 5:

$$\begin{aligned}\big|\mathrm{S}_3(1,-1)\big| &= q+2+\sum_{b\in\mathbb{F}_q}\eta_{\mathbb{F}_q}\Big(1\cdot\big(b^2+b+1\big)^2\Big) = q+2+\Big(q-\Big|\big\{b\in\mathbb{F}_q \mid b^2+b+1=0\big\}\Big|\Big)\eta_{\mathbb{F}_q}(1)\\ &= q+2+\Big(q-\big(1+\eta_{\mathbb{F}_q}(-3)\big)\Big)\cdot 1 = 2q+1-\eta_{\mathbb{F}_q}(-3) = 2q+1-\mathrm{res}_q(3).\end{aligned}$$

Otherwise, if $(c_1,c_2)\neq(1,-1)$, then by the first part of Theorem 5 we get

$$\big|\mathrm{S}_3(c_1,c_2)-q\big| = \Big|2+\sum_{b\in\mathbb{F}_q}\eta_{\mathbb{F}_q}\big(L(b)\big)\Big| \le 2+\Big|\sum_{b\in\mathbb{F}_q}\eta_{\mathbb{F}_q}\big(L(b)\big)\Big| \le 2+(4-1)\sqrt{q} = O(\sqrt{q}),$$

implying that $\mathrm{S}_3(c_1,c_2) = q+O(\sqrt{q})$. This finishes the case when q is odd.

Now suppose that $q = 2^k$. Then, again by part (iv) of Lemma 2 and the case $t = 2$ we have

$$\begin{aligned}
\mathrm{S}_3(c_1, c_2) &= 2(q+1) - \sum_{\substack{b \in \mathbb{F}_q^* \setminus \{c_1\} \\ b^2 + b(1+c_1+c_2) + c_1 = 0}} 1 \\
&\quad - \sum_{\substack{b \in \mathbb{F}_q^* \setminus \{c_1\} \\ b^2 + b(1+c_1+c_2) + c_1 \neq 0}} \left(1 - (-1)^{\mathrm{Tr}_{k,2}\left(\frac{b(b+c_1)^2}{(b^2+b(1+c_1+c_2)+c_1)^2}\right)}\right) \\
&= q + 4 + \sum_{\substack{b \in \mathbb{F}_q^* \setminus \{c_1\} \\ b^2 + b(1+c_1+c_2) + c_1 \neq 0}} (-1)^{\mathrm{Tr}_{k,2}\left(\frac{b(b+c_1)^2}{(b^2+b(1+c_1+c_2)+c_1)^2}\right)}.
\end{aligned}$$

Put

$$f(b) = b(b+c_1)^2 \text{ and } g(b) = (b^2 + b(1+c_1+c_2) + c_1)^2, .$$

and note that both have degree at most 4. Accordingly,

$$\begin{aligned}
\mathrm{S}_3(c_1, c_2) &= q + 4 + \sum_{\substack{b \in \mathbb{F}_q^* \setminus \{c_1\} \\ g(b) \neq 0}} (-1)^{\mathrm{Tr}_{k,2}\left(\frac{f(b)}{g(b)}\right)} \\
&= q + 4 - (-1)^{\mathrm{Tr}_{k,2}\left(\frac{f(0)}{g(0)}\right)} - (-1)^{\mathrm{Tr}_{k,2}\left(\frac{f(c_1)}{g(c_1)}\right)} + \sum_{\substack{b \in \mathbb{F}_q \\ g(b) \neq 0}} (-1)^{\mathrm{Tr}_{k,2}\left(\frac{f(b)}{g(b)}\right)} \\
&= q + 2 + \sum_{\substack{b \in \mathbb{F}_q \\ g(b) \neq 0}} (-1)^{\mathrm{Tr}_{k,2}\left(\frac{f(b)}{g(b)}\right)}.
\end{aligned}$$

To bound the sum we want to use Theorem 6 from the Appendix. It is straightforward to check (see Claim 1 in the Appendix) that the rational function $\frac{f(b)}{g(b)}$ is degenerate if and only if $(c_1, c_2) = (1, 1)$, in which case we have $\mathrm{Tr}_{k,2}\left(\frac{f(b)}{g(b)}\right) = 0$ for every $b \in \mathbb{F}_q, g(b) \neq 0$.

Accordingly, if $(c_1, c_2) = (1, 1)$, then

$$\begin{aligned}
\mathrm{S}_3(1, -1) &= q + 2 + \sum_{\substack{b \in \mathbb{F}_q \\ g(b) \neq 0}} (-1)^0 = 2q + 2 - \left|\left\{b \in \mathbb{F}_q \mid b^2 + b + 1 = 0\right\}\right| \\
&= 2q + 2 - \left(1 + (-1)^{\mathrm{Tr}_{k,2}(1)}\right) = 2q + 1 - (-1)^k = 2q + 1 - \mathrm{res}_3(q).
\end{aligned}$$

Otherwise, if $(c_1, c_2) \neq (1, 1)$, then by Theorem 6 we get

$$\left|\mathrm{S}_3(c_1, c_2) - q\right| = \left|2 + \sum_{\substack{b \in \mathbb{F}_q \\ g(b) \neq 0}} (-1)^{\mathrm{Tr}_{k,2}\left(\frac{f(b)}{g(b)}\right)}\right| \leq 2 + \left|\sum_{\substack{b \in \mathbb{F}_q \\ g(b) \neq 0}} (-1)^{\mathrm{Tr}_{k,2}\left(\frac{f(b)}{g(b)}\right)}\right| \leq 2 + a\sqrt{q},$$

for some positive constant $a \in \mathbb{R}$ (independent of q), implying that $\left|\mathrm{S}_3(c_1, c_2)\right| = q + O(\sqrt{q})$.

For $t = 4$ we use part (iv) of Lemma 2 and the case $t = 3$.

$$\begin{aligned}\mathrm{S}_4(c_1, c_2) &= 2\left(q^2+q+1\right) - \sum_{b\in\mathbb{F}_q^*\setminus\{-c_1\}} \left|\mathrm{S}_3\left(b, \frac{bc_2}{b+c_1}\right)\right| \\ &= 2\left(q^2+q+1\right) - \mathrm{S}_3\left(1, \frac{c_2}{1+c_1}\right) - \sum_{b\in\mathbb{F}_q^*\setminus\{-c_1,1\}} \left|\mathrm{S}_3\left(b, \frac{bc_2}{b+c_1}\right)\right| \\ &= 2\left(q^2+q+1\right) - O(q) - (q-3)\cdot\left(q+O(\sqrt{q})\right) = q^2 + O\left(q^{1.5}\right)\end{aligned}$$

Note that in the above estimate it was crucial that we could use that for most values of b, the value of $\left|S_3\left(b, \frac{bc_2}{b+c_1}\right)\right|$ is asymptotically q.

For $t \geq 5$ we can apply induction with base case $t = 4$. The induction step is the same as above, only that now we do not need to distinguish between cases. Indeed, suppose that the statement holds for all $5 \leq t' < t$ and consider the general case. By part (iv) of Lemma 2 and the induction hypothesis for $t' = t-1$ we obtain

$$\begin{aligned}\mathrm{S}_t(c_1, c_2) &= 2\left(q^{t-2}+\cdots+1\right) - \sum_{b\in\mathbb{F}_q^*\setminus\{-c_1\}} \left|S_{t-1}\left(b, \frac{bc_2}{b+c_1}\right)\right| \\ &= 2\left(q^{t-2}+\cdots+1\right) - (q-2)\cdot\left(q^{t-3}+O\left(q^{t-3.5}\right)\right) = q^{t-2}+O\left(q^{t-2.5}\right).\end{aligned}$$

This finishes the proof of part (b).

3.2 Proof of part (a) of Theorem 2

In this subsection we prove part (a) of Theorem 2 by giving a relatively elementary argument using resultants. Consider the multivariate equation system

$$f_i(Y_1, \ldots, Y_t) = \prod_{j=1}^{t}(Y_j - C_{i,j}) - a_i = 0,\ i \in [3], \tag{10}$$

where $C_{i,j} = -A_i^{q^{j-1}}$ for $i \in [3]$ and $j =\in [t]$. By the identity

$$N(A+B) = \prod_{j=1}^{t}(A+B)^{q^{j-1}} = \prod_{j=1}^{t}(A^{q^{j-1}} + B^{q^{j-1}})$$

we have that for every solution $Y \in \mathbb{F}_{q^t}$ of our original system the vector $\left(Y, Y^q, \ldots, Y^{q^{t-1}}\right) \in \left(\mathbb{F}_{q^t}\right)^t$ is a solution of (10). These are all distinct, hence, to prove part (a) of Theorem 2, it will be enough to show that (10) has at most $6\left(q^{t-3}+\cdots+q+1\right)$ solutions.

For polynomials $p(z) = p_n z^n + \cdots + p_1 z + p_0$ and $r(z) = r_m z^m + \cdots + r_1 z + r_0$ of degree n and m respectively, in the variable z over some field $\mathbb{F}$, their *Sylvester matrix* is the $(n+m)\times(n+m)$ matrix $\mathrm{Syl}(p, r) = \{s_{i,j}\}_{i,j\in[n+m]}$ with entries

$$s_{i,j} = \begin{cases} p_{n+i-j} & \text{if } 1 \leq i \leq m \\ r_{i-j} & m+1 \leq i \leq m+n \\ 0 & \text{otherwise} \end{cases}.$$

For an example consider Figure 1. An important property of the Sylvester matrix is that the degree of the greatest common divisor of p and r is $n+m-\mathrm{rank}(\mathrm{Syl}(p, r))$, in particular if p and r have a common root, then the determinant of $\mathrm{Syl}(p, r)$, also called the *resultant* of p and r, is 0. This holds true even if $p_n = 0$ or $r_m = 0$, that is, when n and m are only upper bounds on the degree of p and r. (See e.g. [43].) Now if p

$$\begin{pmatrix} p_4 & p_3 & p_2 & p_1 & p_0 & 0 & 0 \\ 0 & p_4 & p_3 & p_2 & p_1 & p_0 & 0 \\ 0 & 0 & p_4 & p_3 & p_2 & p_1 & p_0 \\ r_3 & r_2 & r_1 & r_0 & 0 & 0 & 0 \\ 0 & r_3 & r_2 & r_1 & r_0 & 0 & 0 \\ 0 & 0 & r_3 & r_2 & r_1 & r_0 & 0 \\ 0 & 0 & 0 & r_3 & r_2 & r_1 & r_0 \end{pmatrix}$$

Figure 1: The Sylvester matrix for $n = 4$ and $m = 3$

and r are multivariate polynomials in the variables $Y_1, \ldots, Y_n$ over some field F, then we can write them as univariate polynomials in Y_n, and consider their Sylvester matrix (now with entries from $\mathbb{F}[Y_1, \ldots, Y_{n-1}]$). We will call the determinant of this matrix the *Sylvester resultant* of p and r with respect to Y_n, and denote it by $\mathrm{Res}_{Y_n}(p, r)$. Note that $\mathrm{Res}_{Y_n}(p, r)$ is a polynomial in the variables $Y_1, \ldots, Y_{n-1}$. From the above property of the Sylvester matrix it follows that if $(C_1, \ldots, C_n)$ is a common root of p and r, then $(C_1, \ldots, C_{n-1})$ is a root of $\mathrm{Res}_{Y_n}(p, r)$.

Let us now return to the polynomials $f_1, f_2, f_3 \in \mathbb{F}_{q^t}[Y_1, \ldots, Y_t]$. Our plan is to compute $g_i = \mathrm{res}_{Y_t}(f_i, f_3)$ for $i = 1, 2$ and then $g = \mathrm{Res}_{Y_{t-1}}(g_1, g_2)$. Then by the above argument, if $(C_1, \ldots, C_t) \in (\mathbb{F}_{q^t})^t$ is a common root of f_1, f_2, and f_3, then $(C_1, \ldots, C_{t-2}) \in (\mathbb{F}_{q^t})^{t-2}$ is a root of g.

For the computation for $i \in [3]$ we introduce

$$h_i = h_i(Y_1, \ldots, Y_{t-2}) = \prod_{j=1}^{t-2} (Y_j - C_{i,j}),$$

and rewrite f_i as univariate linear polynomial in Y_t:

$$f_i = (h_i \cdot (Y_{t-1} - C_{i,t-1})) \cdot Y_t - (h_i \cdot C_{i,t}(Y_{t-1} - C_{i,t-1}) + b_i)\,.$$

Then for $i = 1, 2$ we have

$$\begin{aligned} g_i =& \mathrm{Res}_{Y_t}(f_i, f_3) = \begin{vmatrix} h_i \cdot (Y_{t-1} - C_{i,t-1}) & -\{h_i \cdot C_{i,t}(Y_{t-1} - C_{i,t-1}) + b_i\} \\ h_3 \cdot (Y_{t-1} - C_{3,t-1}) & -\{h_3 \cdot C_{3,t}(Y_{t-1} - C_{3,t-1}) + b_3\} \end{vmatrix} \\ =& \begin{vmatrix} h_i \cdot (Y_{t-1} - C_{i,t-1}) & -h_i \cdot C_{i,t}(Y_{t-1} - C_{i,t-1}) \\ h_3 \cdot (Y_{t-1} - C_{3,t-1}) & -h_3 \cdot C_{3,t}(Y_{t-1} - C_{3,t-1}) \end{vmatrix} + \begin{vmatrix} h_i \cdot (Y_{t-1} - C_{i,t-1}) & -b_i \\ h_3 \cdot (Y_{t-1} - C_{3,t-1}) & -b_3 \end{vmatrix} \\ =& h_i \cdot h_3 \cdot (Y_{t-1} - C_{i,t-1})(Y_{t-1} - C_{3,t-1}) \begin{vmatrix} 1 & -C_{i,t} \\ 1 & -C_{3,t} \end{vmatrix} - h_i \cdot b_3 (Y_{t-1} - C_{i,t-1}) \\ & + h_3 \cdot b_i (Y_{t-1} - C_{3,t-1}). \end{aligned}$$

That is, $g_i = c_{i,2} Y_{t-1}^2 + c_{i,1} Y_{t-1} + c_{i,0}$ is a quadratic polynomial in Y_{t-1} with coefficients

$$\begin{aligned} c_{i,2} &= h_i \cdot h_3 \cdot \begin{vmatrix} 1 & -C_{i,t} \\ 1 & -C_{3,t} \end{vmatrix}, \\ c_{i,1} &= -h_i \cdot h_3 \cdot (C_{i,t-1} + C_{3,t-1}) \begin{vmatrix} 1 & -C_{i,t} \\ 1 & -C_{3,t} \end{vmatrix} - h_i \cdot b_3 + h_3 \cdot b_i, \\ c_{i,0} &= h_i \cdot h_3 \cdot C_{i,t-1} C_{3,t-1} \begin{vmatrix} 1 & -C_{i,t} \\ 1 & -C_{3,t} \end{vmatrix} + h_i \cdot b_3 C_{i,t-1} - h_3 \cdot b_i C_{3,t-1}. \end{aligned}$$

Hence the resultant of g_1 and g_2 is the four-by-four determinant

$$g = \mathrm{Res}_{Y_{t-1}}(g_1, g_2) = \begin{vmatrix} c_{1,2} & c_{1,1} & c_{1,0} & 0 \\ 0 & c_{1,2} & c_{1,1} & c_{1,0} \\ c_{2,2} & c_{2,1} & c_{2,0} & 0 \\ 0 & c_{2,2} & c_{2,1} & c_{2,0} \end{vmatrix}.$$

Note that each $c_{i,j}$ is a quadratic polynomial in each of the variables $Y_1, \dots, Y_{t-2}$. In particular the degree of g in any of the variables is at most 8. It turns out that this bound can be reduced.

Lemma 3. *For $1 \le a \le t-2$ the coefficient of Y_a^8 in g is 0.*

Proof. The coefficient in question is clearly the determinant we get by replacing $c_{i,j}$ everywhere in the determinant formula for g with the coefficient of Y_a^2 in it. As

$$\begin{aligned}
\operatorname{coeff}(Y_a^2, c_{i,2}) &= \frac{h_i}{Y_a - C_{i,a}} \cdot \frac{h_3}{Y_a - C_{3,a}} \cdot \begin{vmatrix} 1 & -C_{i,t} \\ 1 & -C_{3,t} \end{vmatrix}, \\
\operatorname{coeff}(Y_a^2, c_{i,1}) &= -\frac{h_i}{Y_a - C_{i,a}} \cdot \frac{h_3}{Y_a - C_{3,a}} \cdot (C_{i,t-1} + C_{3,t-1}) \begin{vmatrix} 1 & -C_{i,t} \\ 1 & -C_{3,t} \end{vmatrix} \\
\operatorname{coeff}(Y_a^2, c_{i,0}) &= \frac{h_i}{Y_a - C_{i,a}} \cdot \frac{h_3}{Y_a - C_{3,a}} \cdot C_{i,t-1}C_{3,t-1} \begin{vmatrix} 1 & -C_{i,t} \\ 1 & -C_{3,t} \end{vmatrix},
\end{aligned}$$

we have

$$\begin{aligned}
\operatorname{coeff}(Y_a^8, g) &= \begin{vmatrix} \operatorname{coeff}(Y_a^2, c_{1,2}) & \operatorname{coeff}(Y_a^2, c_{1,1}) & \operatorname{coeff}(Y_a^2, c_{1,0}) & 0 \\ 0 & \operatorname{coeff}(Y_a^2, c_{1,2}) & \operatorname{coeff}(Y_a^2, c_{1,1}) & \operatorname{coeff}(Y_a^2, c_{1,0}) \\ \operatorname{coeff}(Y_a^2, c_{2,2}) & \operatorname{coeff}(Y_a^2, c_{2,1}) & \operatorname{coeff}(Y_a^2, c_{2,0}) & 0 \\ 0 & \operatorname{coeff}(Y_a^2, c_{2,2}) & \operatorname{coeff}(Y_a^2, c_{2,1}) & \operatorname{coeff}(Y_a^2, c_{2,0}) \end{vmatrix} \\
&= \left(\frac{h_1}{Y_a - C_{1,a}}\right)^2 \left(\frac{h_2}{Y_a - C_{2,a}}\right)^2 \left(\frac{h_3}{Y_a - C_{3,a}}\right)^4 \begin{vmatrix} 1 & -C_{1,t} \\ 1 & -C_{3,t} \end{vmatrix}^2 \begin{vmatrix} 1 & -C_{2,t} \\ 1 & -C_{3,t} \end{vmatrix}^2 \cdot D,
\end{aligned}$$

where

$$D = \begin{vmatrix} 1 & -(C_{1,t-1} + C_{3,t-1}) & C_{1,t-1}C_{3,t-1} & 0 \\ 0 & 1 & -(C_{1,t-1} + C_{3,t-1}) & C_{1,t-1}C_{3,t-1} \\ 1 & -(C_{2,t-1} + C_{3,t-1}) & C_{2,t-1}C_{3,t-1} & 0 \\ 0 & 1 & -(C_{2,t-1} + C_{3,t-1}) & C_{2,t-1}C_{3,t-1} \end{vmatrix}.$$

Note that D is just the Sylvester resultant of the two quadratic univariate polynomials $(Y - C_{1,t-1})(Y - C_{3,t-1})$ and $(Y - C_{2,t-1})(Y - C_{3,t-1})$. However, these two have $C_{3,t-1}$ as a common zero and hence their Sylvester resultant is 0. This implies that the coefficient of Y_a^8 in g is 0. □

To reduce the effective degree of g further, observe that h_3 can be factored out from both $c_{2,2}$ and $c_{1,2}$, which are the non-zero entries of the first column of the determinant defining g. Hence $g = h_3 \cdot g^*$ for some polynomial $g^* \in \mathbb{F}_{q^t}[Y_1, \dots, Y_{t-2}]$. Since h_3 is linear in each variable, the degree of g^* in every variable is at most six.

If $(C_1, \dots, C_t)$ is a common zero of f_1, f_2, and f_3, then, as the b_is are non-zero, we have $C_j \neq C_{i,j}$, for $i \in [3]$ and $j \in [t]$. In particular $h_3(C_1, \dots, C_{t-2}) \neq 0$. On the other hand, by the properties of the Sylvester resultant, we must have $g(C_1, \dots, C_{t-2}) = 0$. This implies that $g^*(C_1, \dots, C_{t-2}) = 0$.

Denote by $\tilde{g}$ the univariate polynomial that we obtain by substituting $Y_i = Y^{q^{j-1}}$ in g^* for $j \in [t-2]$. By the degree bounds on g^* we get that the degree of $\tilde{g}$ is at most $6\left(1 + q + q^2 + \cdots + q^{t-3}\right)$, in particular it has at most that many roots. Now if X is a solution to the original system, then $\left(X, X^q, \dots, X^{q^{t-1}}\right)$ is a common root of the f_is, hence $\left(X, X^q, \dots, X^{q^{t-3}}\right)$ is a root of g^* and so X is a root of $\tilde{g}$. Consequently the number of solution to the original system is also bounded by $6\left(1 + q + q^2 + \cdots + q^{t-3}\right)$.

3.3 Three equations with six solutions

This subsection is devoted to proving part (b) of Theorem 2. Meanwhile, on the way we also give a proof of Theorem 3. As in the remainder of this subsection we will solely consider the case $t = 3$, to simplify notation, from now on we will simply write N for the norm function N_3.

For two equations we already proved that in some degenerate cases the system of norm equations has twice as many solutions as in the rest of the cases. Heuristically one could think that when considering three equations it should be easier to find a system with 6 solutions among those which contain such exceptional subsystems. That is the reason that we look at the particular system

$$\mathrm{N}(X) = 1, \qquad \mathrm{N}(X+1) = -1, \qquad \mathrm{N}(X+A) = -1, \tag{11}$$

where A is a non-identity element of norm 1 in $\mathbb{F}_{q^3}$.

In what follows, we will work out the details of the heuristics described above. We start by investigating the exceptional norm equation system

$$\mathrm{N}(X) = 1, \qquad \mathrm{N}(X+1) = -1, \tag{12}$$

and the algebraic structure of its solution set $\mathrm{S}_3(1,-1)$. In particular, in what follows, we prove Theorem 3. To do so, first we observe that in this case the corresponding polynomial $f_{3,1,-1}$ can be written in a product form.

$$\begin{aligned} f_{3,1,-1}(X) &= (X+1)^{q+1}X^{q+1} + (X+1)^{q+1} + X^{q+1} = X^{2q+2} + X^{2q+1} + X^{q+2} + 3X^{q+1} + X^q + X + 1 \\ &= (X^{q+1} + X + 1)\cdot(X^{q+1} + X^q + 1) = h_1(X)\cdot h_2(X). \end{aligned} \tag{13}$$

For $i = 1, 2$ let $\mathcal{H}_i$ denote the set of roots of h_i in $\overline{\mathbb{F}}_q$ and let $\mathcal{N}$ denote the set of elements in $\mathbb{F}_{q^3}$ with norm 1. It is easy to see that $\mathcal{N}$ is an order q^2+q+1 subgroup of the multiplicative group $\mathbb{F}_{q^3}^*$.

For general c_1, c_2 the polynomial f_{3,c_1,c_2} can have roots which are not in $\mathrm{S}_3(c_1,c_2)$. The first part of Theorem 3 states that this does not happen when $(c_1,c_2) = (1,-1)$. We prove this in the following lemma.

Lemma 4. *For every prime power $q \geq 2$ we have*

$$S_3(1,-1) = \big\{X \in \overline{\mathbb{F}}_{q^3} \mid h_1(X)\cdot h_2(X) = 0\big\} = \mathcal{H}_1 \cup \mathcal{H}_2.$$

Proof. By (13) and by part (i) of Lemma 2 we have $\mathrm{S}_3(1,-1) \subseteq \mathrm{R}_4(1,-1) = \big\{X \in \overline{\mathbb{F}}_{q^3} \mid h_1(X)\cdot h_2(X) = 0\big\}$.

Now let $X \in \overline{\mathbb{F}}_q$ be such that $h_1(X)\cdot h_2(X) = 0$. Then either

$$h_1(X) = 0 \text{ and hence } X^q = -\frac{1}{X+1} = u(X), \quad \text{or} \quad h_2(X) = 0 \text{ and hence } X^q = -\frac{X+1}{X} = v(X).$$

In the first case

$$X^{q^2} = u\big(u(X)\big) = -\frac{1}{-\frac{1}{X+1}+1} = v(X)$$

and

$$X^{q^3} = u\Big(u\big(u(X)\big)\Big) = u\big(v(X)\big) = -\frac{1}{-\frac{X+1}{X}+1} = X,$$

while in the latter case

$$X^{q^2} = v\big(v(X)\big) = -\frac{-\frac{X+1}{X}+1}{-\frac{X+1}{X}} = u(X)$$

and

$$X^{q^3} = v\Big(v\big(v(X)\big)\Big) = v\big(u(X)\big) = -\frac{-\frac{1}{X+1}+1}{-\frac{1}{X+1}} = X.$$

In particular, in both cases we have $X \in \mathbb{F}_{q^3}$ and $X^q \cdot X^{q^2} = u(X)v(X)$. Accordingly,

$$\mathrm{N}(X) = X \cdot X^q \cdot X^{q^2} = X \cdot u(X) \cdot v(X) = X \cdot \left(-\frac{1}{X+1}\right) \cdot \left(-\frac{X+1}{X}\right) = 1.$$

Similarly, for the norm of $X+1$ we get

$$\begin{aligned}\mathrm{N}(X+1) &= (X+1)(X^q+1)(X^{q^2}+1) = (X+1)(u(X)+1)(v(X)+1)\\ &= (X+1)\cdot\left(-\frac{X+1}{X}+1\right)\cdot\left(-\frac{1}{X+1}+1\right) = -1.\end{aligned}$$

This shows that $X \in \mathrm{S}_3(1,-1)$ and hence $\left\{X \in \overline{\mathbb{F}}_{q^3} \mid h_1(X)\cdot h_2(X) = 0\right\} \subseteq \mathrm{S}_3(1,-1)$. □

Note that Lemma 4, in particular, also shows that $\mathcal{H}_1, \mathcal{H}_2 \subseteq \mathcal{N}$. The second part of Theorem 3 will directly follow from the next proposition where we prove several helpful properties of the sets $\mathcal{H}_i$.

Proposition 2. *(i)* $\mathcal{H}_2 = \mathcal{H}_1^{-1}$.

(ii) Every $A \in \mathcal{N}\setminus\{1\}$ *can be represented uniquely as a product* $A = A_1\cdot A_2$ *of an element* A_1 *of* $\mathcal{H}_1$ *and an element* A_2 *of* $\mathcal{H}_2$. *This representation is given by*

$$A_1 = \frac{A^{q+1}-1}{1-A^q} \qquad \text{and} \qquad A_2 = \frac{A-A^{q+1}}{A^{q+1}-1} \in \mathcal{H}_2. \tag{14}$$

(iii) $\mathcal{H}_1\cap\mathcal{H}_2 = \mathcal{H}_1\cap\mathbb{F}_q = \mathcal{H}_2\cap\mathbb{F}_q = \left\{Y\in\mathbb{F} : Y^2+Y+1=0\right\}$, *in particular*

$$\mathcal{H}_1\cap\mathcal{H}_2 = \begin{cases} \{1\} & \text{if } q\equiv 0 \pmod 3\\ \{\alpha,\alpha^{-1}\},\ \text{where } \alpha^3=1,\alpha\neq 1 & \text{if } q\equiv 1 \pmod 3\\ \emptyset & \text{if } q\equiv 2 \pmod 3\end{cases}.$$

(iv) $\mathcal{H}_1$ *and* $\mathcal{H}_2$ *are invariant under the Frobenius map* $X\to X^q$.

Proof. The statement of (i) follows from the simple fact $h_2\left(\frac{1}{X}\right) = \frac{h_1(X)}{X^{q+1}}$.

For (ii) we first show the uniqueness of the representation of the form (14). Suppose that $A\in\mathcal{N}\setminus\{1\}$ and $A = A_1\cdot A_2$ with $A_1\in\mathcal{H}_1$ and $A_2 = \frac{A}{A_1}\in\mathcal{H}_2$. Then

$$A_1^{q+1}+A_1+1 = 0 \qquad \text{and} \qquad \left(\frac{A}{A_1}\right)^{q+1}+\left(\frac{A}{A_1}\right)^q+1 = 0.$$

By expressing A_1^q from the two equations we obtain

$$\frac{A_1+1}{A_1} = \frac{A^{q+1}}{A_1}+A^q.$$

Solving for A_1 gives that the only possibility is

$$A_1 = \frac{A^{q+1}-1}{1-A^q}.$$

This gives uniqueness and the stated formula (14) for $A_2 = \frac{A}{A_1}$ as well. It remains to verify that $A_i\in\mathcal{H}_i$. We consider first A_1. Using $\mathrm{N}(A) = A^{q^2+q+1} = 1$ we get

$$\begin{aligned}h_1(A_1) &= \frac{A^{q+1}-1}{1-A^q}\cdot\left(\frac{A^{q+1}-1}{1-A^q}\right)^q+\frac{A^{q+1}-1}{1-A^q}+1 = \frac{A^{q+1}-1}{1-A^q}\cdot\frac{A^{q^2+q}-1}{1-A^{q^2}}+\frac{A^q\cdot(A-1)}{1-A^q}\\ &= \frac{\frac{1}{A^{q^2}}-1}{1-A^q}\cdot\frac{\frac{1}{A}-1}{1-A^{q^2}}+\frac{\frac{1}{A^{q^2+1}}(A-1)}{1-A^q} = \frac{1-A}{A^{q^2+1}\cdot(1-A^q)}+\frac{A-1}{A^{q^2+1}\cdot(1-A^q)} = 0,\end{aligned}$$

and hence $A\in\mathcal{H}_1$. The verification of $A_2\in\mathcal{H}_2$ is a similar calculation that we leave to the reader.

To see the desired equalities of sets in (iii) note that for an element $Y\in\mathbb{F}_{q^3}$ we have $h_1(Y) = h_2(Y)$ if and only $Y = Y^q$, which happens if and only if $Y\in\mathbb{F}_q$. Then for $3|q$ we have $X^2+X+1 = (X-1)^2$, while otherwise the non-trivial third-roots of unity are in $\mathbb{F}_q$ if and only if $3|q-1$.

The statement of (iv) is a direct consequence of the fact that the Frobenius map is an automorphism of the field $\mathbb{F}_{q^3}$that fixes $\mathbb{F}_q$. □

Note that as in an order q^2+q+1 multiplicative group any difference set must have size $q+1$, Theorem 3, in particular, also implies that $|\mathcal{H}_1| = |\mathcal{H}_1| = q+1$, which in turn is equivalent to the polynomials h_1, h_2 splitting into linear factors over $\mathbb{F}_{q^3}$.

Next we connect our main interest, the solution set of (11), to the solution set of (12), and hence to the difference sets $\mathcal{H}_1$, $\mathcal{H}_2$.

Proposition 3. *An element $Y \in \mathbb{F}_{q^3}$ is a solution of (11) with parameter $A \in \mathcal{N} \setminus \{1\}$ if and only if Y and $\frac{A}{Y}$ are both contained in $\mathcal{H}_1 \cup \mathcal{H}_2$.*

Proof. By Lemma 4 we know that Y and $\frac{A}{Y}$ are both contained in $\mathcal{H}_1 \cup \mathcal{H}_2$ if and only if they are both solutions of (12). We show that this is equivalent to Y being a solution of (11).

Suppose first that $Y \in \mathbb{K}$ is a solution of (11). Then a fortiori Y is a solution of (12) and $Y \neq 0$. Also,

$$\mathrm{N}\left(\frac{A}{Y}\right) = \frac{\mathrm{N}(A)}{\mathrm{N}(Y)} = \frac{1}{1} = 1 \qquad \text{and} \qquad \mathrm{N}\left(\frac{A}{Y}+1\right) = \mathrm{N}\left(\frac{A+Y}{Y}\right) = \frac{\mathrm{N}(A+Y)}{\mathrm{N}(Y)} = \frac{-1}{1} = -1,$$

hence $\frac{A}{Y}$ is also a solution of (12).

Conversely, assume that Y and $\frac{A}{Y}$ are both solutions of (12). Then, in particular, Y satisfies the first two equations from (11), as for the third one we have

$$\mathrm{N}(Y+A) = \mathrm{N}\left(Y\left(1+\frac{A}{Y}\right)\right) = \mathrm{N}(Y)\,\mathrm{N}\left(\frac{A}{Y}+1\right) = 1 \cdot -1 = -1,$$

and hence Y is a solution of (11). □

By the previous proposition, when trying to solve (11) we will be looking for product representations $Y \cdot \frac{A}{Y}$ of the element A involving factors from $\mathcal{H}_1 \cup \mathcal{H}_2$. To prove part (b) of Theorem 2 we will need to find an element $A \in \mathcal{N} \setminus \{1\}$ that has three such product representations $A = B_1C_1 = B_2C_2 = B_3C_3$, such that the six elements $B_1, C_1, B_2, C_2, B_3, C_3 \in \mathcal{H}_1 \cup \mathcal{H}_2$ are all distinct. For this we will crucially use that $\mathcal{H}_1$ and $\mathcal{H}_2 = \mathcal{H}_1^{-1}$ are difference sets in $\mathcal{N}$ and inverses of each other.

Recall that if $\mathcal{D}$ is any difference set in some multiplicative group G then every element $A \in G \setminus \{1\}$ has a unique representation, called mixed representation, as a product $B \cdot C = A$ such that one of B and C is from $\mathcal{D}$ and the other is from $\mathcal{D}^{-1}$. In the next propositions we summarize our knowledge about other product representations. To this end we will call a product $B \cdot C = A$ a *$\mathcal{D}$-representation* of the element $A \in G$ if both B and C are from $\mathcal{D}$.

Proposition 4. *Let $\mathcal{D}$ be an arbitrary difference set in some multiplicative group G. Then every $A \in G$ has at most one $\mathcal{D}$-representation.*

Proof. Let us assume that $D_1D_2 = D_3D_4$ for some $D_1, D_2, D_3, D_4 \in \mathcal{D}$. Then $D_1D_3^{-1} = D_4D_2^{-1}$, and this, by the difference set property, is either 1 or we have $D_1 = D_4$ and $D_2 = D_3$: in any case $\{D_1, D_2\} = \{D_3, D_4\}$. □

The explicit descriptions of our specific difference sets allow us to characterize when an $\mathcal{H}_i$-representation with distinct factors exists.

Proposition 5. *Let $q \geq 3$ be an odd prime power.*

(i) $A \in \mathcal{N}$ has an $\mathcal{H}_1$-representation with different factors if and only if $\left(A+1-A^{q+1}\right)^2 - 4A$ is a non-zero square in $\mathbb{F}_{q^3}$. In particular, $A \in \mathcal{H}_1$ has an $\mathcal{H}_1$-representation with different factors if and only if A^2+A+1 is a non-zero square in $\mathbb{F}_{q^3}$.

(ii) $A \in \mathcal{N}$ has an $\mathcal{H}_2$-representation with different factors if and only if $(A^{q+1}+A^q-1)^2 - 4A^{q+1}$ is a non-zero square in $\mathbb{F}_{q^3}$. In particular, $A \in \mathcal{H}_2$ has an $\mathcal{H}_2$-representation with different factors if and only if A^2+A+1 is a non-zero square in $\mathbb{F}_{q^3}$.

Proof. As the proof of the two parts is analogous, below we only present the one of (i).

Suppose first that $A \in \mathcal{N}$ has an $\mathcal{H}_1$-representation. This means that there is an element $Y \in \mathbb{F}_{q^3}$ such that Y and $\frac{A}{Y}$ are both roots of h_1, i.e.

$$h_1(Y) = Y^{q+1} + Y + 1 = 0 \qquad \text{and} \qquad h_1\left(\frac{A}{Y}\right) = \left(\frac{A}{Y}\right)^q \cdot \frac{A}{Y} + \frac{A}{Y} + 1 = 0.$$

After expressing Y^q from both equations, letting them being equal and clearing denominators we obtain $Y^2 + \left(A + 1 - A^{q+1}\right) \cdot Y + A = 0$. Clearly, the role of Y and $\frac{A}{Y}$ can be switched, which means that both Y and $\frac{A}{Y}$ are roots of the quadratic equation

$$X^2 + \left(A + 1 - A^{q+1}\right) \cdot X + A = 0. \tag{15}$$

This is possible only if the discriminant

$$D = \left(A + 1 - A^{q+1}\right)^2 - 4A$$

is a nonzero square in $\mathbb{F}_{q^3}$.

For the other direction suppose that $D = \left(A + 1 - A^{q+1}\right)^2 - 4A$ is a nonzero square in $\mathbb{F}_{q^3}$, i.e. there is some element $G \in \mathbb{F}_{q^3}^*$ such that $D = G^2$. Then we know that the quadratic equation in (15) has two different roots, namely $X_\pm = \frac{A^{q+1} - A - 1 \pm G}{2}$. Clearly, $X_+ \cdot X_- = A$, so to finish the proof it is enough to show that $X_\pm \in \mathcal{H}_1$, i.e. $h_1(X_\pm) = 0$.

Using $N(A) = A^{q^2+q+1} = 1$ we have

$$\begin{aligned} D^q &= \left(\left(A + 1 - A^{q+1}\right)^2 - 4A\right)^q = \left(A^q + 1 - A^{q^2+q}\right)^2 - 4A^q = \\ &= \left(A^q + 1 - \frac{1}{A}\right)^2 - 4A^q = \frac{1}{A^2}\left(\left(A^{q+1} + A - 1\right)^2 - 4A^{q+2}\right) = \\ &= \frac{1}{A^2}\left(\left(A + 1 - A^{q+1}\right)^2 - 4A\right) = \frac{1}{A^2} D. \end{aligned}$$

Then

$$\left(\frac{G^q}{G}\right)^2 = \frac{(G^2)^q}{G^2} = \frac{D^q}{D} = \frac{\frac{1}{A^2} D}{D} = \frac{1}{A^2}$$

and hence $\frac{G^q}{G} = \pm\frac{1}{A}$. However

$$N\left(\frac{G^q}{G}\right) = \frac{G^q}{G} \cdot \left(\frac{G^q}{G}\right)^q \cdot \left(\frac{G^q}{G}\right)^{q^2} = \frac{G^q}{G} \cdot \frac{G^{q^2}}{G^q} \cdot \frac{G}{G^{q^2}} = 1$$

which, excludes $\frac{G^q}{G} = -\frac{1}{A}$. Therefore $G^q = \frac{1}{A} G$. As a consequence we get

$$\begin{aligned} (X_\pm)^q = \phi\left(\frac{A^{q+1} - A - 1 \pm G}{2}\right) &= \frac{A^{q^2+q} - A^q - 1 \pm G^q}{2} = \\ &= \frac{\frac{1}{A} - A^q - 1 \pm \frac{1}{A} G}{2} = \frac{1}{A} X_\pm + \frac{1 - A^{q+1}}{A}. \end{aligned}$$

Now we are ready to substitute $X_\pm$ into h_1.

$$\begin{aligned} h_1(X_\pm) = X_\pm \cdot (X_\pm)^q + X_\pm + 1 &= X_\pm \cdot \left(\frac{1}{A} X_\pm + \frac{1 - A^{q+1}}{A}\right) + X_\pm + 1 = \\ &= \frac{1}{A}\left(X_\pm^2 + \left(A + 1 - A^{q+1}\right) \cdot X_\pm + A\right) = 0, \end{aligned}$$

where at the last equality we just used that $X_\pm$ are the roots of (15).

To finish the proof just note that when $A \in \mathcal{H}_1$ then $(A + 1 - A^{q+1})^2 - 4A$ simplifies to $4(A^2 + A + 1)$, which, is a non-zero square in $\mathbb{F}_{q^3}$ if and only $A^2 + A + 1$ is such. $\square$

For the elements of $\mathcal{H}_i$ the existence of a $\mathcal{H}_{3-i}$-representation follows directly.

Proposition 6. *If $A \in \mathcal{H}_i$ then its unique $\mathcal{H}_{3-i}$-representation is given by $\frac{1}{A^q} \cdot \frac{1}{A^{q^2}} = A$.*

Proof. On the one hand, as $A \in \mathcal{H}_i \subseteq \mathcal{N}$, we have that $A = \frac{N(A)}{A^{q^2+q}} = \frac{1}{A^q} \cdot \frac{1}{A^{q^2}}$. On the other hand, by Proposition 2, part (i) we have $\frac{1}{A} \in \mathcal{H}_{3-i}$, and so by Proposition 2, part (iv) we have $\frac{1}{A^q} = \left(\frac{1}{A}\right)^q \in \mathcal{H}_{3-i}$ and $\frac{1}{\psi(A)} = \left(\frac{1}{A^q}\right)^q \in \mathcal{H}_{3-i}$. The uniqueness follows from Proposition 4. □

To continue, we will need to split the proof into three different cases based on the remainder of $p \pmod 3$.

3.3.1 Case I: $p \equiv 2 \pmod 3$

In this subsection we settle the case when $p \equiv 2 \pmod 3$, in particular the case of even characteristic.

First we show the existence of six solutions when q is congruent to 2 modulo 3 (as opposed to p). Recall that to do so we aim to find an element $A \in \mathcal{N} \setminus \{1\}$, which, next to its unique mixed representation $A = A_1 \cdot A_2$ with $A_1 \in \mathcal{H}_1$ and $A_2 \in \mathcal{H}_2$ (which exists by Proposition 2), also has an $\mathcal{H}_i$-representation $A = B_i \cdot C_i$ for both $i = 1$ and 2, such that $B_i \neq C_i$, and these six elements are all different. Note that the latter follows immediately from the fact that, when $q \equiv 2 \pmod 3$ the sets $\mathcal{H}_1$ and $\mathcal{H}_2$ are disjoint by Proposition 2, part (iii).

In order to find the appropriate element A for which the $\mathcal{H}_i$-representations exist, for a set $\mathcal{H} \subseteq \mathcal{N}$ we define

$$\mathcal{H}^* := \{B \cdot C \ : \ B, C \in \mathcal{H}, \ B \neq C\}$$

to be the set of its pairwise products from distinct factors, and show that $\mathcal{H}_1^* \cap \mathcal{H}_2^*$ is not empty. An element from this intersection is clearly suitable.

First note that by Proposition 5, part (ii) the pairwise products of the elements of $\mathcal{H}_i$ are all distinct, hence the cardinality of $\mathcal{H}_i^*$ is $\binom{|\mathcal{H}_i|}{2} = \frac{q^2+q}{2}$. Both $\mathcal{H}_1^*$ and $\mathcal{H}_2^*$ are subsets of the (q^2+q)-element set $\mathcal{N} \setminus \{1\}$. For this note that $\mathcal{H}_i$ is contained in $\mathcal{N}$, which is closed under multiplication, and that $1 \notin \mathcal{H}_i^*$ since $\mathcal{H}_i$ is disjoint from its inverse $\mathcal{H}_{3-i}$ by our assumption on q and Proposition 2, part (iii). Hence the only way $\mathcal{H}_1^*$ and $\mathcal{H}_2^*$ could be disjoint is if their union is $\mathcal{N} \setminus \{1\}$. In this case however it would also hold that

$$\sigma(\mathcal{N} \setminus \{1\}) = \sigma(\mathcal{H}_1^*) + \sigma(\mathcal{H}_2^*), \tag{16}$$

where $\sigma(\mathcal{S})$ denotes the sum of the elements of a subset $\mathcal{S} \subseteq \mathbb{F}_{q^3}$. On the one hand the set $\mathcal{N}$ is the collection of all q^2+q+1 roots in $\mathbb{F}_{q^3}$ of the polynomial $X^{q^2+q+1} - 1$ and so $\sigma(\mathcal{N})$ is (-1) times the coefficient of X^{q^2+q} in this polynomial, which is 0. From this we obtain that $\sigma(\mathcal{N} \setminus \{1\}) = -1$. On the other hand $\mathcal{H}_i$ is the set of all $q+1$ roots in $\mathbb{F}_{q^3}$ of the polynomial $h_i(X)$, hence $\sigma(\mathcal{H}_i^*)$ is the coefficient of X^{q-1} in $h_i(X)$, which is 0 for $q > 2$. We arrived to a contradiction, as the left hand side of (16) is (-1), while the right hand side is 0. This settles the case when $q \equiv 2 \pmod 3$.

For the more general case, next note that $\mathbb{F}_{q^6}$ is a cubic extension of $\mathbb{F}_{q^2}$ and the norm of an element $B \in \mathbb{F}_{q^3} \subseteq \mathbb{F}_{q^6}$ is the same, irrespective in which of the two fields we compute it: $\mathrm{N}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(B) = \mathrm{N}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^2}}(B)$.

This means that if for an element $A \in \mathbb{F}_{q^3}$ with $\mathrm{N}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(A) = 1$ the system (11) with the norm function $\mathrm{N}_{\mathbb{F}_{q^3}/F_q}$ has six distinct solutions $X_1, \ldots, X_6 \in \mathbb{F}_{q^3}$, then the very same six elements are also solutions of the the system (11) with the norm function $\mathrm{N}_{\mathbb{F}_{q^6}/F_{q^2}}$.

Now let $p \equiv 2 \pmod 3$ be a prime and let $q = p^k = p^{\ell 2^m}$ be an arbitrary power where ℓ is odd. Then from above we get the required six distinct solutions when $m = 0$ and $p^\ell > 2$. By repeated application of the previous observation, the statement also follows for any positive integer m and $p^\ell > 2$. These include all the powers when $p > 2$.

When $p = 2$ then only those powers are included where $\ell \geq 3$. So we are left with prime powers of the form 2^{2^m}. To settle these last cases one first resolves the problem when the prime power is $2^{2^2} = 16$ and then uses the above squaring trick to deduce the case of arbitrary $2^{2^m} = 16^{2^{m-2}}$.

For $q = 16$ we have found the appropriate $A \in \mathbb{F}_{16^3}$ of norm 1, for which the system (11) has six distinct solution with the aid of a computer. To describe this example, let U be the primitive element of $\mathbb{F}_{16^3}^*$ whose minimal polynomial over $\mathbb{F}_2$ is $X^{12} + X^7 + X^6 + X^5 + X^3 + X + 1$, and consider the system

$$\mathrm{N}(X) = 1, \qquad \mathrm{N}(X+1) = 1, \qquad \mathrm{N}(X + U^{405}) = 1.$$

By Magma Calculator [20] it is easily verified that $A = U^{405}$ is in $\mathcal{N} \setminus \{1\}$, and that the system has indeed six solutions, namely $U^{1725}, U^{2775}, U^{3435} \in \mathcal{H}_1$ and $U^{1065}, U^{2130}, U^{2370} \in \mathcal{H}_2$ with

$$A = U^{1065} \cdot U^{3435} = U^{1725} \cdot U^{2775} = U^{2130} \cdot U^{2370}.$$

3.3.2 Case II: $p = 3$

In this subsection we settle the case when $p = 3$. Our strategy is the same as in the previous subsection, but now we do this in two steps. First we find an element that has both $\mathcal{H}_1$- and $\mathcal{H}_2$-representation, but in one of them the factors are not distinct.

Lemma 5. *For $i = 1$ or 2 there is an element $C \in \mathcal{H}_i \setminus \{1\}$, such that C^2 has an $\mathcal{H}_{3-i}$-representation $C^2 = B \cdot E$ with distinct factors $B \neq E$.*

Proof. We want to find a $C \in \mathcal{H}_i \setminus \{1\}$ for $i = 1$ or 2, such that C^2 has an $\mathcal{H}_{3-i}$-representation with different elements B and E. This happens exactly if one of the formulas in Proposition 5 is a nonzero square in $\mathbb{F}_{q^3}$ when we substitute $A = C^2$. It turns out that after simplifying the substituted formula of (i) using $h_2(C) = C^{q+1} + C^q + 1 = 0$ and clearing its square denominator we obtain the very same expression $D(C)$ as after simplifying the substituted formula of (ii) using $h_1(C) = C^{q+1} + C + 1 = 0$ and clearing its square denominator:

$$\begin{aligned} D = D(C) &= \left(C^2(C+1)^2 + (C+1)^2 - C^2\right)^2 - 4(C+1)^4C^2 = \\ &= \left(C^2 + 3C + 1\right) \cdot \left(C^2 + C + 1\right) \cdot \left(C^2 + C - 1\right) \cdot \left(C^2 - C - 1\right). \end{aligned}$$

We aim to find an element $C \in \mathcal{H}_1 \cup \mathcal{H}_2 \setminus \{1\}$ for which D is a square in $\mathbb{F}_{q^3}$, or equivalently, $N(D)$ is a square in $\mathbb{F}_q$.

As it turns out the factors of $N(D)$ can be conveniently expressed using the trace $\mathrm{Tr}_{3,q}(C) = C + C^q + C^{q^2} =: \tau$ of C:

$$\begin{aligned} N(C^2 + 3C + 1) &= -\tau^2 - 3\tau - 1, \\ N(C^2 + C + 1) &= \tau^2 + 3\tau + 9, \\ N(C^2 + C - 1) &= \tau^2 + 3\tau + 1, \\ N(C^2 - C - 1) &= -\tau^2 - 3\tau - 1, \end{aligned}$$

and so

$$N(D) = (-\tau^2 - 3\tau - 1)^2(\tau^2 + 3\tau + 9)(\tau^2 + 3\tau + 1).$$

In characteristic 3 this expression is a square if and only if $\tau^2 + 1$ is a square. Using Theorem 5.18 from [46] we get that

$$\sum_{Y \in \mathbb{F}_q} \eta_{\mathbb{F}_q}(Y^2 + 1) = -\eta_{\mathbb{F}_q}(1) = -1,$$

Therefore, as $Y^2 + 1 = 0$ has at most two solutions, for at least $\dfrac{q-3}{2}$ elements $y \in \mathbb{F}_q$ the expression $Y^2 + 1$ is a square.

This ensures the existence of many good "traces", which we can use to construct many good C, as we now show that the trace function is a 3-to-1 function on $\mathcal{H}_1 \cup \mathcal{H}_2 \setminus \{1\}$. That is, if $\mathrm{Tr}(C_1) = \mathrm{Tr}(C_2)$ for

$C_1, C_2 \in \mathcal{H}_1 \cup \mathcal{H}_2 \setminus \{1\}$ then C_1 and C_2 are conjugates of each other. For this we note that the minimal polynomial of an element C of $\mathcal{H}_1 \cup \mathcal{H}_2 \setminus \{1\}$ can be expressed just by the trace τ of C:

$$m_\tau(X) = (X - C)(X - C^q)(X - C^{q^2}) = X^3 - \tau X^2 - (\tau + 3)X - 1.$$

Hence if C_1 and C_2 have the same trace, then they have the same minimal polynomial.

Consequently there are exactly $\frac{|\mathcal{H}_1 \cup \mathcal{H}_2 \setminus \{1\}|}{3} = \frac{2q}{3}$ elements in $\mathbb{F}_q^*$ that are traces of some element in $\mathcal{H}_1 \cup \mathcal{H}_2 \setminus \{1\}$.

In conclusion, if $q > 9$ then there are at least $\left(\frac{2q}{3} + \frac{q-3}{2}\right) - q = \frac{q-9}{6} > 0$ elements $t \in \mathbb{F}_q$ which are traces of an element C from $\mathcal{H}_1 \cup \mathcal{H}_2 \setminus \{1\}$, and for which $t^2 + 1$, and hence also $D = D(C)$, is a square. This completes the proof for $q > 9$.

Otherwise, by our assumption on q, we are left with the case $q = 9$. Then we can directly find a $\tau \in \mathbb{F}_9$ such that it is the trace of an element $C \in \mathcal{H}_1 \cup \mathcal{H}_2 \setminus \{1\}$ and $\tau^2 + 1$ is a nonzero square in $\mathbb{F}_9$. In fact $\tau = -1$ will do. First note that $\tau^2 + 1 = 1 + 1 = 2$ is in $\mathbb{F}_3$ and hence is a square in its quadratic extension $\mathbb{F}_9$. Now, to finish the argument it is enough to show that $m_{-1}(X) = X^3 + X^2 + X - 1$ is the minimal polynomial of some $C \in \mathcal{H}_1 \cup \mathcal{H}_2 \setminus \{1\}$ over $\mathbb{F}_9$, because then we automatically have $\mathrm{Tr}(C) = \tau = -1$. It is immediate that $m_{-1}(X)$ is irreducible over $\mathbb{F}_3$, hence it can not have a root in $\mathbb{F}_9$, and therefore it is irreducible over $\mathbb{F}_9$. Next consider the polynomial $h_1(X)$ for $q = 3$. Then (when computed over $\mathbb{F}_3$) we have

$$h_1(X) = X^4 + X + 1 = (X - 1)(X^3 + X^2 + X - 1) = (X - 1)m_{-1}(X),$$

which in view of Lemma 4 means that the roots of $m_{-1}(X)$ solve the system (12) with norm function $\mathrm{N}_{\mathbb{F}_{3^3}/\mathbb{F}_3}$. But then, as we have seen earlier, the roots of $m_{-1}(X)$ also solve the system (12) with norm function $\mathrm{N}_{\mathbb{F}_{9^3}/\mathbb{F}_9}$, and hence, again by Lemma 4 and the fact $m_{-1}(1) \neq 0$, we have that any root of m_{-1} is in $\mathcal{H}_1 \cup \mathcal{H}_2 \setminus \{1\}$, as desired. □

Let us now fix elements $C \in \mathcal{H}_i \setminus \{1\}$ and $B, E \in \mathcal{H}_{3-i}$ guaranteed by Lemma 5. We show that the element $A := \frac{C}{E}$ is the kind we are looking for. First observe that by Proposition 2, part (i)

$$A = C \cdot \frac{1}{E} = B \cdot \frac{1}{C}$$

provide a $\mathcal{H}_i$- and $\mathcal{H}_{3-i}$-representation of A, respectively. Note furthermore that as $(\mathcal{H}_i \setminus \{1\}) \cap \mathcal{H}_{3-i} = \emptyset$, we have $C \neq E$ and hence $A \neq 1$. Consequently, by Proposition 2, part (ii) there exists a unique mixed representation $A = A_1 \cdot A_2$ with $A_i \in \mathcal{H}_i$.

Next we show that these six elements from the representations are all distinct. By Proposition 3 these elements then provide six distinct solutions of (11).

Lemma 6. *The elements $A_i, C, \frac{1}{E} \in \mathcal{H}_i$ and $A_{3-i}, \frac{1}{C}, B \in \mathcal{H}_{3-i}$ are all distinct.*

Proof. For the distinctness first we establish that none of the six elements is 1. This is certainly true for C and $\frac{1}{C}$ by the choice of C in Lemma 5. Now assume that B or E is 1, say $B = 1$ (the argument in the case $E = 1$ is analogous). On the one hand, as $E \in \mathcal{H}_{3-i}$, by Proposition 6 E has a unique $\mathcal{H}_i$-representation: $E = \frac{1}{E^q} \cdot \frac{1}{E^{q^2}}$. On the other hand $E = B \cdot E = C \cdot C$ is also a $\mathcal{H}_i$-representation of E, so by the uniqueness we must have $E^q = \frac{1}{C} = E^{q^2} = \phi(E^q)$, and thus $E^q \in \mathbb{F}_q$ and $E^q = \frac{1}{C} \in \mathcal{H}_{3-i}$. That means $\phi(E) = E^q \in \mathbb{F}_q \cap \mathcal{H}_{3-i} = \mathcal{H}_1 \cap \mathcal{H}_2 = \{1\}$ by Proposition 2, part (iii), which is only possible if $E = 1$. This contradicts $C \neq 1$ and implies $B, E \neq 1$. Finally assume that A_1 or A_2 is equal to 1, say $A_1 = 1$. Then $A_1 \cdot A_2 = A = B \cdot \frac{1}{C}$ are two $\mathcal{H}_2$-representations of A. By uniqueness either B or C should be 1, which is a contradiction by the above.

Since none of the six elements is 1 and by part (iii) of Proposition 2 $\mathcal{H}_1 \cap \mathcal{H}_2 = \{1\}$, we established that

$$\{A_i, C, \frac{1}{E}\} \cap \{A_{3-i}, B, \frac{1}{C}\} = \emptyset.$$

We are left to show that $\left|\{A_i, C, \frac{1}{E}\}\right| = 3$ and $\left|\{A_{3-i}, B, \frac{1}{C}\right| = 3$. Since they are proved analogously we present just the first one.

If $A_i = C$, then $A_{3-i} = \frac{1}{E}$, which is a contradiction as $A_{3-i} \in \mathcal{H}_{3-i}$ and $\frac{1}{E} \in \mathcal{H}_i$ and none of them is 1. If $A_i = \frac{1}{E}$, then $A_{3-i} = C$, which is a contradiction similarly as $A_{3-i} \in \mathcal{H}_{3-i}$ and $C \in \mathcal{H}_i$ and none of them is 1. Finally, suppose that $C = \frac{1}{E}$. Then we have $B = C^2 \cdot \frac{1}{E} = C^3$, which is a contradiction as $B \in \mathcal{H}_{3-i} \setminus \{1\}$ and $C^3 \in \mathcal{H}_i \setminus \{1\}$ because the polynomial h_i is defined over $\mathbb{F}_3$, hence if $h_i(C) = 0$, then $h_i(C^3) = 0$ as well. □

3.3.3 Case III: $q \equiv 1 \pmod 3$ odd

The last case we consider is when $q \equiv 1 \pmod 3$. Note that this, in particular, covers the cases when $p \equiv 1 \pmod 3$. We remark that the proof below can be adapted whenever $p \geq 5$, but for simplicity we only present it for the particular case $q \equiv 1 \pmod 3$.

As in the previous subsection we aim again to find an A which has three distinct representations, but instead of looking for it in $\mathcal{N} \setminus \{1\}$ we will restrict ourselves to $\mathcal{H}_1 \cup \mathcal{H}_2$. With such a choice of A, Proposition 2 still guarantees a mixed representation $A = A_1 \cdot A_2$ with $A_i \in \mathcal{H}_i$, but now, if say $A \in \mathcal{H}_i$ then Proposition 6 also guarantees an $\mathcal{H}_{3-i}$ representation $A = \frac{1}{A^q} \cdot \frac{1}{A^{q^2}}$. Therefore, what is left is to find an $\mathcal{H}_i$-representation $A = B \cdot C$ with different factors $B, C \in \mathcal{H}_i$. According to Proposition 5 such a representation exist exactly if $A^2 + A + 1$ is a non-zero square in $\mathbb{F}_{q^3}$. To look for such an element, it will be convenient to embed the set $\mathcal{H}_1 \cup \mathcal{H}_2$ into a more structured ambiance.

For this, let us fix a non-trivial third root of unity $\alpha \in \mathbb{F}_q$ (which exists when $3 \mid q-1$) and consider the linear fractional transformation $\gamma : \mathbb{F}_{q^3} \setminus \{\alpha\} \to \mathbb{F}_{q^3}$, defined by

$$\gamma(Z) = \frac{Z - \alpha^{-1}}{Z - \alpha}.$$

Further let us denote by G multiplicative groups of $3(q-1)$-st roots of unity in $\mathbb{F}_{q^3}$, i.e.

$$G = \left\{ Y \in \mathbb{F}_{q^3}^* \mid Y^{3(q-1)} = 1 \right\}.$$

Note that as $q \equiv 1 \pmod 3$, G is well defined and has size $3(q-1)$.

Lemma 7. *If $q \equiv 1 \pmod 3$ then the map $Z \mapsto \gamma(Z)$ is a bijection from the symmetric difference $\mathcal{H}_1 \triangle \mathcal{H}_2 = (\mathcal{H}_1 \setminus \mathcal{H}_2) \cup (\mathcal{H}_2 \setminus \mathcal{H}_1)$ to $G \setminus \mathbb{F}_q^*$.*

Proof. Let $Z \in \mathcal{H}_1 \triangle \mathcal{H}_2$. As $\alpha, \alpha^{-1} \in \mathcal{H}_1 \cap \mathcal{H}_2$ the value $\gamma(Z)$ well defined and nonzero. We aim to show that $\gamma(Z) \in G \setminus \mathbb{F}_q^*$, which happens exactly if $\gamma(Z)^{q-1} \neq 1$ but $\gamma(Z)^{3(q-1)} = 1$. Without loss of generality we may assume that $Z \in \mathcal{H}_1 \setminus \mathcal{H}_2$, the other case can be handled analogously.

$$\gamma(Z)^q = \frac{(Z - \alpha^{-1})^q}{(Z - \alpha)^q} = \frac{Z^q - \alpha^{-q}}{Z^q - \alpha^q} = \frac{Z^q - \alpha^{-1}}{Z^q - \alpha}$$

As $Z \in \mathcal{H}_1$, we have $Z^q = -\frac{Z+1}{Z}$, and hence, using $1 + \alpha + \alpha^{-1} = 0$ and $\alpha^2 = \alpha^{-1}$ we obtain

$$\gamma(Z)^q = \frac{-\frac{Z+1}{Z} - \alpha^{-1}}{-\frac{Z+1}{Z} - \alpha} = \frac{Z\alpha^{-1} + Z + 1}{Z\alpha + Z + 1} = \frac{Z\alpha - 1}{Z\alpha^{-1} - 1} = \frac{Z - \alpha^{-1}}{Z - \alpha} \cdot \alpha^{-1} = \gamma(Z) \cdot \alpha^{-1}.$$

Therefore, $\gamma(Z)^{q-1} = \alpha^{-1} \neq 1$, but $\gamma(Z)^{3(q-1)} = (\alpha^{-1})^3 = 1$, as desired.

γ is clearly injective because it is a nontrivial fractional linear map, and hence to verify that γ is indeed a bijection between the two sets it is enough to show that they are of the same size. On the one hand, as $\mathbb{F}_q^*$ is fully contained in G, the set $G \setminus \mathbb{F}_q^*$ has size $3(q-1) - (q-1) = 2(q-1)$. On the other hand, as $|\mathcal{H}_i| = q+1$ and $\mathcal{H}_1 \cap \mathcal{H}_2 = \{\alpha, \alpha^{-1}\}$, the set $\mathcal{H}_1 \triangle \mathcal{H}_2$ has the same size. □

Recall that we want to find an element $A \in \mathcal{H}_1 \cup \mathcal{H}_2$ for which $A^2 + A + 1$ is a non-zero square in $\mathbb{F}_{q^3}$. This will be done using the following lemma.

Lemma 8. *If $q \equiv 1 \pmod 3$, then for every $A \in \mathcal{H}_1 \triangle \mathcal{H}_2$, we have*

$$\eta_{\mathbb{F}_{q^3}}(A^2 + A + 1) = \eta_{\mathbb{F}_{q^3}}(\gamma(A)),$$

that is, $A^2 + A + 1$ is a square in $\mathbb{F}_{q^3}$ if and only if $\gamma(A)$ is such.

Proof. Let $r \in \overline{\mathbb{F}}_q$ and $s \in \overline{\mathbb{F}}_q$ be a square root of A^2+A+1 and $\gamma(A)$, respectively. Then $\eta_{\mathbb{F}_{q^3}}(A^2+A+1) = 1$ if and only if $r^{q^3-1} = 1$ (i.e., $r \in \mathbb{F}_{q^3}$) and $\eta_{\mathbb{F}_{q^3}}(\gamma(A)) = 1$ if and only if $s^{q^3-1} = 1$ (i.e., $s \in \mathbb{F}_{q^3}$).

As α and α^{-1} are the roots of the polynomial $X^2 + X + 1$, we have

$$r^2 = A^2 + A + 1 = (A - \alpha^{-1}) \cdot (A - \alpha) = \gamma(A) \cdot (A - \alpha)^2 = s^2 \cdot (A - \alpha)^2.$$

Then, since $q^3 - 1$ is even and $A - \alpha \in \mathbb{F}_{q^3}$, we have

$$r^{q^3-1} = (s \cdot (A - \alpha))^{q^3-1} = s^{q^3-1} \cdot (A - \alpha)^{q^3-1} = s^{q^3-1},$$

and so they equal 1 at the same time, as required. □

Now, to select the element we are looking for, fix a generator g of the cyclic group G and let $A \in \mathcal{H}_1 \triangle \mathcal{H}_2$ for which $\gamma(A) = g^2$. Note that then the previous lemma ensures that A^2+A+1 is a square and in particular we have $A \notin \mathbb{F}_q$. This way we obtained the three different representations discussed before. The only thing we are left with is to show that the six elements $A_1, A_2, \frac{1}{A^q}, \frac{1}{A^{q^2}}, B, C$ are all different. We already know that $B \neq C$ and, as $A \notin \mathbb{F}_q$, we also have $\frac{1}{A^q} \neq \frac{1}{A^{q^2}}$. Now suppose we have $A_1 = A_2$. This would imply that $A_1 = A_2 \in \mathcal{H}_1 \cap \mathcal{H}_2 \subseteq \mathbb{F}_q$, and hence A belongs to $\mathbb{F}_q$, a contradiction. Next suppose that the mixed and the $\mathcal{H}_{3-i}$ representations would coincide. This would be only possible if $\frac{1}{A^q}$ or $\frac{1}{A^{q^2}}$ would belong to $\mathcal{H}_1 \cap \mathcal{H}_2 \subseteq \mathbb{F}_q$ which in turn would imply $A \in \mathbb{F}_q$, again a contradiction. The same argument also shows that the $\mathcal{H}_1$ and $\mathcal{H}_2$-representations must be different. At last suppose that the mixed and the $\mathcal{H}_i$ representations coincide, say we have $A_1 = B$ and $A_2 = C$. Then one these elements would belong to $\mathcal{H}_1 \cap \mathcal{H}_2$ and hence would be a non-trivial third root of unity, and therefore A would be of the form αY or $\alpha^{-1}Y$ for some $Y \in \mathcal{H}_1 \cup \mathcal{H}_2$. The contradiction in this case wil follow from the lemma below.

Lemma 9. *If $q \equiv 1 \pmod 3$ and $A \in \mathcal{H}_1 \triangle \mathcal{H}_2$ then $\alpha A, \alpha^{-1}A \notin \mathcal{H}_1 \cup \mathcal{H}_2$.*

Proof. Assume to the contrary that $cA \in \mathcal{H}_1 \cup \mathcal{H}_2$ for $c = \alpha$ or α^{-1}. As $A \notin \mathbb{F}_q$ we must then also have $cA \notin \mathbb{F}_q$, so by Lemma 7 both $\gamma(A)$ and $\gamma(cA)$ belong to $G \setminus \mathbb{F}_q^*$. By definition

$$\gamma(\alpha A) = \frac{\alpha A - \alpha^{-1}}{\alpha A - \alpha} = \frac{A - \alpha^{-2}}{A - 1} = \frac{A - \alpha}{A - 1} \quad \text{and}$$
$$\gamma(\alpha^{-1} A) = \frac{\alpha^{-1} A - \alpha^{-1}}{\alpha^{-1} A - \alpha} = \frac{A - 1}{A - \alpha^2} = \frac{A - 1}{A - \alpha^{-1}},$$

which in particular implies that $\gamma(A) \cdot \gamma(\alpha A) \cdot \gamma(\alpha^{-1} A) = 1$. Since two of the three factors are in G, so must be the third.

By the definition of G, the three elements $\gamma(A)^3$, $\gamma(\alpha A)^3$ and $\gamma(\alpha^{-1}A)^3$ all have to be roots of the polynomial $X^{q-1} - 1 = 0$ and hence belong to $\mathbb{F}_q$. A straightforward but tedious computation shows that A can be expressed as

$$A = \frac{\alpha \gamma(A)^3 \gamma(\alpha A)^3 + \alpha^2 \gamma(\alpha A)^3 + 1}{1 - \alpha^2 \gamma(A)^3 \gamma(\alpha A)^3 - \alpha \gamma(\alpha A)^3}.$$

Since all the ingredients were shown to be in $\mathbb{F}_q$, so has to be A, a contradiction. □

3.4 Proof of Corollary 1 and 2

We start by proving the key ingredient, Proposition 1, which connects common degrees of vertex sets to solution sets of norm equations.

Proof of Proposition 1. By definition, the common neighbourhood of T is the solution set of the system

$$\mathrm{N}_{t-1}(V_i + X) = v_i x, \quad i \in [\ell]. \tag{17}$$

By dividing the first $\ell - 1$ equations with the last one and applying the straightforward change of variable $Y = \frac{1}{X+V_\ell}$ we arrive at the norm equation system

$$\mathrm{N}_{t-1}(A_i + Y) = a_i, \quad i \in [\ell - 1] \tag{18}$$

where for $i \in [\ell - 1]$ the parameters $A_i = A_i(T)$ and $a_i = a_i(T)$ are as described in the statement. This transformation also shows that if (Y, y) is a solution to (17), then $\Phi\big((Y, y)\big) = \frac{1}{Y+V_\ell}$ is a solution of (18). Note that $\Phi\big((Y, y)\big)$ is always well-defined, as $N(Y + Y_\ell) = v_\ell \cdot y \neq 0$, and hence $Y + V_\ell \neq 0$. By definition $\Phi\big((Y, y)\big) \neq 0$ and so we get $\Phi(\mathcal{N}(T)) \subseteq \mathrm{S}_{t-1}\big(A(T)\big) \setminus \{0\}$.

As $\mathcal{N}(\mathcal{N}(T)) \supseteq T \neq \emptyset$, the neighborhood $\mathcal{N}(T)$ is generic, so Φ is injective on $\mathcal{N}(T)$.

For the surjectivity of Φ let $Z \in \mathrm{S}_{t-1}\big(A(T)\big)\setminus\{0\}$ and consider the vertex $\left(\frac{1}{Z} - V_\ell, \frac{1}{v_\ell \cdot N(Z)}\right) \in \Phi^{-1}(Z)$. Next we show that this vertex belongs to $\mathcal{N}(T)$. Indeed, for $i \in [\ell - 1]$ we have

$$N\left(V_i + \left(\frac{1}{Z} - V_\ell\right)\right) = N\left(\frac{1}{A_i} + \frac{1}{Z}\right) = N\left(\frac{Z + A_i}{A_i Z}\right) = \frac{a_i}{N(A_i)N(Z)} = \frac{1}{v_\ell \cdot N(Z)} \cdot v_i,$$

and for $i = \ell$ we have

$$N\left(V_\ell + \left(\frac{1}{Z} - V_\ell\right)\right) = N\left(\frac{1}{Z}\right) = \frac{1}{v_\ell \cdot N(Z)} \cdot v_\ell.$$

To finish the proof just note that $0 \in \mathrm{S}_{t-1}\big(A(T)\big)$ if and only if $N(A_i) = a_i = \frac{v_i}{v_\ell} \cdot N(A_i)$ for every $i \in [\ell-1]$, which in turn is equivalent to $v_1 = v_2 = \cdots = v_\ell$, i.e. to $\xi(T) = 1$. □

Now Corollary 1 is a direct consequence of Theorem 1 and Proposition 1. To prove Corollary 2 we need a few more details.

First we connect solutions of general norm equation systems with three equations to four adjacencies in the projective norm-graph.

Lemma 10. *Let $P = \big\{(A_1, a_1), (A_2, a_2), (A_3, a_3)\big\} \subseteq \mathbb{F}_{q^3}^* \times \mathbb{F}_q^*$ and $Y \in S_3(P) \setminus \{0\}$. Then for any $(V, v) \in \mathbb{F}_{q^3} \times \mathbb{F}_q^*$ in the projective norm graph $\mathrm{NG}(q, 4)$ the vertex $\left(\frac{1}{Y} - V, \frac{1}{v\,\mathrm{N}(Y)}\right)$ is adjacent to all the vertices*

$$\left(\frac{1}{A_1} + V, \frac{a_1 v}{\mathrm{N}(A_1)}\right), \qquad \left(\frac{1}{A_2} + V, \frac{a_2 v}{\mathrm{N}(A_2)}\right), \qquad \left(\frac{1}{A_3} + V, \frac{a_3 v}{\mathrm{N}(A_3)}\right), \qquad (V, v).$$

Proof. We check all the adjacencies from the statement. For the first three vertices, using $\mathrm{N}(Y + A_i) = a_i$, we have

$$\mathrm{N}\left(\frac{1}{A_i} + V + \frac{1}{Y} - V\right) = \mathrm{N}\left(\frac{Y + A_i}{A_i Y}\right) = \frac{\mathrm{N}(Y + A_i)}{\mathrm{N}(A_i Y)} = \frac{a_i}{\mathrm{N}(A_i)\,\mathrm{N}(Y)} = \frac{a_i v}{\mathrm{N}(A_i)} \cdot \frac{1}{v \cdot \mathrm{N}(Y)}.$$

For the last vertex we have

$$\mathrm{N}\left(V + \frac{1}{Y} - V\right) = \mathrm{N}\left(\frac{1}{Y}\right) = v \cdot \frac{1}{v \cdot \mathrm{N}(Y)},$$

as requested. □

By Theorem 2 there exists an element $A \in \mathcal{N} \setminus \{1\}$ such that for the triple $U = \big\{(0,1),(1,-1),(A,-1)\big\} \subseteq \mathbb{F}_{q^3}^* \times \mathbb{F}_q^*$ we have $\big|S_3(U)\big| = 6$. If we choose any element $C \in \mathbb{F}_{q^3} \setminus \big(\{0,-1,-A\} \cup S_3(U)\big)$ and $D \in \mathbb{F}_{q^3}^*$, then the transformed system with parameters

$$U_{C,D} = \left\{ \left(\frac{C}{D}, \frac{1}{\mathrm{N}(D)}\right), \left(\frac{C+1}{D}, -\frac{1}{\mathrm{N}(D)}\right), \left(\frac{C+A}{D}, -\frac{1}{\mathrm{N}(D)}\right) \right\}$$

will still have 6 solutions. Moreover, by the choice of C we made sure that all three of the first coordinates and all the 6 solutions are nonzero. Therefore, we can apply Lemma 10 to obtain that for any $(V,v) \in \mathbb{F}_{q^3} \times \mathbb{F}_q^*$ the set

$$T_{C,D,V,v} = \left\{ \left(\frac{D}{C} + V, \frac{v}{\mathrm{N}(C)}\right), \left(\frac{D}{C+1} + V, -\frac{v}{\mathrm{N}(C+1)}\right), \left(\frac{D}{C+A} + V, -\frac{v}{\mathrm{N}(C+A)}\right), (V,v) \right\}$$

of vertices has 6 common neighbours in $\mathrm{NG}(q,4)$, namely

$$\mathcal{N}(T_{C,D,V,v}) = \left\{ \left(\frac{1}{Y} - V, \frac{1}{v\,\mathrm{N}(Y)}\right) : Y \in S_3(U_{C,D}) \right\}.$$

Note that for any (ordered) quadruple Q of points of $\mathrm{NG}(q,4)$ there is at most one selection of C, D, V and v such that $Q = T_{C,D,V,v}$. Furthermore, in order for these 24 adjacencies to indeed give rise to a $K_{4,6}$ in $NG(q,4)$, we need to make sure that none of them represents a loop. If q is even, then $\mathrm{NG}(q,4)$ has no loop edges, so all the participating $4+6$ vertices are by default different, and they form a $K_{4,6}$. Now assume q is odd and assume C, D, v to be fixed. We call an element $V \in \mathbb{F}_{q^3}$ *bad* if for this element some of first in $T_{C,D,V,v}$ coincides with some other first coordinate in $\mathcal{N}(T_{C,D,V,v})$. Note that if we forbid bad elements for our choice of V then already the first coordinates forbid a loop to appear. However, for every vertex from $T_{C,D,V,v}$ and any other vertex from $T_{C,D,V,v}$ there exists exactly one element V which makes their first coordinates coincide, and therefore, together there are at most 24 bad elements.

In conclusion we get at least $(q^3-9)(q^3-1)(q^3-24)(q-1) = (1+o(1))q^{10}$ quadruples[4] which host a $K_{4,6}$. Some of these still might coincide, but at most with multiplicity $4! = 24$, so altogether we still get $\Omega(q^{10})$ different copies of $K_{4,6}$.

3.5 Proof of Theorem 4 and Corollary 3 and 4

We start by introducing some further notation. Denote by $\Delta_d(q,t)$ and $\delta_d(q,t)$, respectively, the largest and smallest possible common degree of a generic d-tuple of vertices in the projective norm graph $\mathrm{NG}(q,t)$. For $d = 0$, we set $\Delta_0(q,t) = \delta_0(q,t) = |V(\mathrm{NG}(q,t)|$.

Now let H be a simple ℓ-degenerate graph and suppose that $t \geq 3$. To simplify notation put $v = v(H)$ and $m = e(H)$. Further let $v_1, \ldots, v_v$ be an ordering of the vertices of H witnessing its ℓ-degeneracy, i.e. every vertex v_i has at most ℓ neighbours in $\{v_1, \ldots, v_{i-1}\}$. For $1 \leq i \leq v$ put $\mathcal{N}_i = \mathcal{N}(v_i) \cap \{v_1, \ldots, v_{i-1}\}$ and $d_i = |\mathcal{N}_i|$, in particular $\mathcal{N}_1 = \emptyset$ and $d_1 = 0$. With this notation for our ordering we have $d_i \leq \ell$ for $1 \leq i \leq v$.

To count the number of labeled copies of H in $\mathrm{NG}(q,t)$ we will embed the vertices of H into $\mathrm{NG}(q,t)$ one-by-one according the above order. Suppose we have already embedded $v_1, \ldots, v_{i-1}$. To embed v_i, we have to choose a vertex from the common neighbourhood T_i of the image of $\mathcal{N}_i$ under this embedding. As T_i is of size d_i, it has at most $\Delta_{d_i}(q,t)$ common neighbours in $\mathrm{NG}(q,t)$, so we have at most $\Delta_{d_i}(q,t)$ choices for v_i. Accordingly

$$X_H(\mathrm{NG}(q,t)) \leq \prod_{i=1}^{v} \Delta_{d_i}(q,t).$$

To obtain a similar lower bound we can repeat the same argument with the extra condition that during the embedding we want every possible set of already embedded vertices of size at most ℓ to be generic. We will

[4]Note that we assume $q \geq 5$, so all factors are positive.

achieve this simply by mapping the vertices of H each time to a vertex of $\mathrm{NG}(q,t)$ with a first coordinate different from all the previous ones.

So suppose that we have already embedded $v_1,\dots,v_{i-1}$ with the desired property. To embed v_i, we have to choose a vertex from the common neighbourhood T_i of the image of $\mathcal{N}_i$ under this embedding whose first coordinate is different from those of the images of $v_1,\dots,v_{i-1}$. The image of N_i is now a generic set of size d_i, it has at least $\delta_{d_i}(q,t)$ common neighbours. To maintain our extra condition, when choosing the image of v_i we have to exclude the common neighbours with first coordinate equal to the first coordinates of the previously selected ones. If $d_i=0$ then this means that we have to exclude $(i-1)(q-1)$ vertices, but there still will be at least $\delta_0(q,t)-(i-1)(q-1)\geq\delta_0(q,t)-vq$ candidates for the image of v_i. If $d_i>0$, then, as $\deg(T_i)\geq d_i>0$, it must be generic set, and hence cannot contain two vertices with the same first coordinate. Therefore, for every previously selected vertex we have to exclude at most one vertex from T_i, and so there still will be at least $\delta_{d_i}(q,t)-(i-1)\geq\delta_{d_i}(q,t)-v$ candidates for the image of v_i. Accordingly we obtain that

$$X_H(\mathrm{NG}(q,t))\geq\prod_{i=1}^{v}\left(\delta_{d_i}(q,t)-v\chi_i\right),$$

where $\chi_i=q$ if $d_i=0$ and $\chi_i=1$ otherwise.

Now to finish the proof of Theorem 4 we will consider two cases.

First suppose $\ell=3$ and $t\geq5$ or $\ell=2$ and $t\geq3$. In both cases by Corollary 1 we know that there exists a positive constant C such that for all $d\leq\ell$ we have

$$|\Delta_d(q,t)-q^{t-d}|,|\delta_d(q,t)-q^{t-d}|\leq Cq^{t-d-\frac{1}{2}}. \tag{19}$$

Recall that by the construction of the order $d_i\leq\ell$ for $i\in[v]$, hence using (19) we get

$$\begin{aligned}X_H(\mathrm{NG}(q,t))&\leq\prod_{i=1}^{v}\Delta_{d_i}(q,t)\leq\prod_{i=1}^{v}\left(q^{t-d_i}+Cq^{t-d_i-\frac{1}{2}}\right)=\left(\prod_{i=1}^{v}q^{t-d_i}\right)\left(1+\frac{C}{\sqrt{q}}\right)^v\\&=q^{t\cdot v-(d_1+\dots d_v)}\left(1+\frac{C}{\sqrt{q}}\right)^v=q^{t\cdot v-m}\left(1+\frac{C}{\sqrt{q}}\right)^v\leq q^{t\cdot v-m}\left(1+C'\frac{v}{\sqrt{q}}\right)\end{aligned}$$

for some appropriate positive constant C', whenever $v=o(\sqrt{q})$. Similarly, again using (19), we get

$$\begin{aligned}X_H(\mathrm{NG}(q,t))&\geq\prod_{i=1}^{v}\left(\delta_{d_i}(q,t)-v\chi_i\right)\geq\prod_{i=1}^{v}\left(q^{t-d_i}-Cq^{t-d_i-\frac{1}{2}}-v\chi_i\right)\\&\geq\prod_{i=1}^{v}\left(q^{t-d_i}-C''q^{t-d_i-\frac{1}{2}}\right)\end{aligned}$$

for some appropriate positive constant $C''\geq C$. Note that for all sets of parameters in the case $d_i=0$ we have $t-\frac{1}{2}\geq\frac{3}{2}$ and in the case $d_i>0$ we have $t-d_i-\frac{1}{2}\geq\frac{1}{2}$, hence, whenever $v=o(\sqrt{q})$,then for given C such a C'' really exists. Then, similarly as before, we get

$$X_H(\mathrm{NG}(q,t))\geq\left(\prod_{i=1}^{v}q^{t-d_i}\right)\left(1-\frac{C''}{\sqrt{q}}\right)^v=q^{t\cdot v-m}\left(1-\frac{C''}{\sqrt{q}}\right)^v\geq q^{t\cdot v-m}\left(1-v\frac{C''}{\sqrt{q}}\right).$$

The two bounds together give that $X_H(\mathrm{NG}(q,t))$ is asymptotically $q^{t\cdot v-m}$ as desired.

Finally suppose $\ell=3$ and $t=4$. In this case, according to Corollary 1, $\Delta_3(q,4)$ and $\delta_3(q,4)$ differ asymptotically by a factor of 2, so the same proof only yields

$$q^{t\cdot v-m}\big(1-o(1)\big)\leq X_H(\mathrm{NG}(q,4))\leq 2^{c(H)}q^{t\cdot v-m}\big(1+o(1)\big),$$

where $c(H)$ is the minimum number of indicies with $d_i=3$ in any witnessing ordering of the vertices of H. Accordingly, this shows that $X_H(\mathrm{NG}(q,4))=\Theta(q^{t\cdot v-m})$ for any H with $v=o(\sqrt{q})$ and $c(H)$ bounded.

This, on the one hand, completes the proof of Theorem 4. On the other hand, as the lower bounds in the two cases are identical, they also conclude Corollary 3. Finally, Corollary 4 can be obtained by combining the lower bound from Corollary 3 with the general upper bound of Alon and Shikhelman from [7].

4 Concluding remarks

Several interesting questions remain open.

1. Common neighbourhoods. Corollary 1 fully describes the common neighbourhoods of sets of vertices of size at most 3. In most cases the number of common neighbours is asymptotically as expected in a uniform random graph with the same edge density. We conjecture that the analogous "ℓ-wise independence" phenomenon occurs for larger sets of vertices as well.

Conjecture 2. *For arbitrary integers $4 \leq \ell < t$ all but $o(n^\ell)$ sets of ℓ vertices in $\mathrm{NG}(q,t)$ have $(1+o(1))q^{t-\ell}$ common neighbours.*

2. Complete bipartite graphs in projective norm graphs. In Corollary 2 we could only find special kinds of copies of $K_{4,6}$, whose number is only roughly q^{10}. We think however, that the number of copies of $K_{4,6}$ in $\mathrm{NG}(q,4)$ should be the same order as their typical number in the random graph of the same edge density.

Conjecture 3. *The number of copies of $K_{4,6}$ in $\mathrm{NG}(q,4)$ is $\Theta(q^{16})$.*

The determination of $s(t)$ is still widely open for $t \geq 5$, when we do not even know whether there is a $K_{t,t}$ in $\mathrm{NG}(q,t)$ for every large enough q. While it is probably more realistic to expect that there are copies of $K_{t,(t-1)!}$ for every $t \geq 5$ and large enough q (besides numerology, i.e. that $s(t) = (t-1)!$ for $t = 2, 3$ and 4, there are also algebro-geometric heuristics pointing towards this), we harbour a slim hope that $t = 4$ was still a special case. At least the graph $\mathrm{NG}(q,4)$ seems quite special, with a unique structure and symmetries, and maybe that alone is responsible for the presence of $K_{4,6}$ subgraphs.

3. Quasirandomness. In Theorem 4 we proved that if $t \geq 4$ then $\mathrm{NG}(q,t)$ is H-quasirandom whenever H is a fixed simple 3-degenerate graph. A positive answer to Conjecture 2 would directly imply a generalization of this result to ℓ-degenerate graphs. It would be also interesting to study what can we say beyond the scope of Conjecture 2, about the containment of fixed small graphs in general. Especially interesting would be the cases of cliques. The so-called clique-graphs of the projective norm graphs were explicitly used by Alon and Pudlák [4] for their constructions for the asymmetric Ramsey problem. They lower bound the clique number $\omega(NG(q,t))$ by the Expander Mixing Lemma, which is probably far from being tight. In this paper we go beyond that and show not only the existence of K_4, but also the K_4-quasirandomness of $\mathrm{NG}(q,t)$ for $t \geq 4$. We are, however, still very far from the understanding of the behaviour of the clique number. Besides its exact determination there are several other intriguing directions. We think that once a "nice" fixed graph H is contained in the projective norm graph for every large enough q, then there are the "right" number of copies of it.

Conjecture 4.
(i) For every $2 \leq t \leq s \leq s(t)$ the projective norm graph $\mathrm{NG}(q,t)$ is $K_{t,s}$-quasirandom.
(ii) If $s \leq \omega(\mathrm{NG}(q,t))$ for every large enough q, then $\mathrm{NG}(q,t)$ is K_s-quasirandom.

Finally, there is very little known about whether there are any characteristic-specific subgraphs. We do not know whether there is any fixed graph H which is contained in projective norm graphs for some characteristic p_1, but it is not contained in them for some other characteristic p_2.

4. Infinite projective norm graphs. The first constructions of dense $K_{t,t}$-free graphs were motivated by simple facts from real Euclidean geometry: two lines of the plane intersect in at most one point; three unit spheres in 3-space intersect in at most two points. Consequently the point/line incidence graph of the Euclidean plane is $K_{2,2}$-free, and the unit-distance graph of the Euclidean 3-space is $K_{3,3}$-free. Furthermore these infinite $K_{t,t}$-free graphs are "dense" in terms of the dimension of the neighborhoods. So when defined

over appropriate finite fields, in a way that the algebra in the proof of their $K_{t,t}$-freeness carries over, their number of edges verifies the tightness of the KST-bound for $t = 2$ and $t = 3$.

The (projective) norm graphs were not constructed this way, yet one can define them over an arbitrary field $\mathbb{F}$ and arbitrary Galois extension $\mathbb{K}$ of degree $t-1$, see Section 5.3 in the Appendix. If $t = 4$ then we know that $\mathrm{NG}(\mathbb{F}, \mathbb{K})$ does not contain $K_{4,7}$ for any field $\mathbb{F}$. After seeing that $\mathrm{NG}(q, 4)$ does contain (many) $K_{4,6}$ for any $q > 4$, it seems plausible to conjecture that the same is true for infinite fields.

5. The tightness of the KST-bound. The tightness of the order of magnitude of the KST-bound is a central question of the area. Conjecture 1 suggests that whatever density is not ruled out by simple double counting, should essentially be possible to realize with a construction. Here we speculate that this might not be the case and offer a counter-conjecture.

In any graph with $cn^{7/4}$ edges, the number of common neighbors of an average 4-tuple is (at least) a constant c' depending on c. If this graph with $cn^{7/4}$ edges is random then this constant average is spread out over $\binom{n}{4}$ distributions that are each approximately Poisson with mean c'. Consequently for any s, a positive constant proportion of 4-tuples have at least s neighbors. In contrast, in any $K_{4,s}$-free construction with $cn^{7/4}$ edges (matching the KST-bound), no 4-tuple can have more than $s-1$ neighbors. So in such constructions each of the Poisson-tails has to be absorbed by the 4-tuples with at most $s-1$ common neighbors. Should such graphs exist for some s, they must be extremely rare, their mere existence has to be a coincidence and should require quite a bit of structure.

In all known constructions (including ARS [5], Brown [21], Bukh [22], Klein [28] and KRS [38]) this is realized using the algebro/geometric notion of dimension and its strong correlation with the cardinality of the corresponding variety: an "everyday" d-dimensional variety over $\mathbb{F}_q$ has roughly $\Theta(q^d)$ points. To achieve that the common neighborhood of four vertices is less than a constant s, one appeals to the geometric intuition that in the four-dimensional space the intersection of four hypersurfaces, that are in general enough position, is 0-dimensional, and hence it is the union of constantly many points. A graph can be defined on a four-dimensional space of roughly $q^4 =: n$ vertices, and the neighborhood of each vertex can be chosen to be some hypersurface, which then have roughly the desired size $q^3 = n^{3/4}$. For a $K_{4,s}$-free graph the intersection of any four of the neighborhood-hypersurfaces should have size $< s$. Now if the neighborhood-hypersurfaces are carefully chosen, so that any four of them are in general enough position, then their intersection is 0-dimensional and hence has size $\Theta(q^0)$, a constant.

How to choose the hypersurfaces and what is this constant? Even though choosing randomly is a generally good strategy (witnessed by the random algebraic construction of Bukh [22]), finding good explicit choices, as it is often the case, is not so straightforward. By the KST-bound the constant bounding the neighborhoods of t-tuples in any graph with $cn^{2-1/t}$ edges is at least $t-1$, and the projective norm graph chooses neighborhoods where they are bounded by not more than $(t-1)!$. The current analysis of the random choice gives an upper bound of $t^{O(t)}$.

Now how small could this constant be? We believe that the presence of some notion of "dimension" in this problem is a necessity and this constant is just going to be in the nature of the geometry of the hypersurface-neighborhoods we have chosen. As such, it will not just be limited by the simple combinatorial restrictions of the KST-bound but also by those of geometry/algebra. And then its extrema should be delivered by a regular, rigid structure with distinctive properties. For $t = 4$ we have seen ample evidence that the projective norm graph $\mathrm{NG}(q, 4)$ fits this bill, and tend to accept it as the limit of what algebra can offer in this realm. Since we know now that $K_{4,6}$ does occur in $\mathrm{NG}(q, 4)$, we conjecture the following.

Conjecture 5. $\mathrm{ex}(n, K_{4,6}) = o(n^{7/4})$.

We note that should this conjecture be true, it of course implies that the KST-bound is not tight for the symmetric case $K_{4,4}$ either. That further implies that $\mathrm{ex}(n, K_{t,t}) = o(n^{2-1/t})$ for every $t \geq 5$; this is the consequence of (an adaptation of) a theorem of Erdős and Simonovits [29].

While we do believe Conjecture 5, at the same time we also think that it is more likely that we see it disproved than proved. For a proof one might need to develop a two step approach. Given a $K_{4,4}$-free graph with $cn^{7/4}$ edges, build up a significant-enough proportion of a pseudo-algebraic/geometric framework

using the neighborhoods as hypersurfaces, with surfaces having appropriate intersection sizes and structure. Then, provided the pseudo-algebra/geometry gives a structure rigid enough, establish the existence of a $K_{4,4}$. Preliminary results in this direction were proven by Blagojevic, Bukh, and Karasev [18] and in this paper.

References

[1] N. Alon, S. Moran, A. Yehudayoff. Sign Rank, VC Dimension and Spectral Gaps. In: V. Feldman, A. Rakhlin, O. Shamir (eds.), Proceedings of COLT'16, Proceedings of Machine Learning Research vol. 49, PMLR, 2016. pp. 47–80. Also: Mathematicheskii Sbornik 208:4–41, 2017.

[2] N. Alon, M. Krivelevich, B. Sudakov. MaxCut in H-Free Graphs. Combinatorics, Probability and Computing 14:629–647, 2005.

[3] N. Alon, M. Krivelevich, B. Sudakov. Turán numbers of bipartite graphs and related Ramsey-type questions. Combinatorics, Probability and Computing 12:477–494, 2003.

[4] N. Alon, P. Pudlák. Constructive lower bounds for off-diagonal Ramsey numbers. Israel Journal of Mathematics 122(1):243–251, 2001.

[5] N. Alon, L. Rónyai, T. Szabó. Norm-graphs: variations and applications. Journal of Combinatorial Theory, Series B 76:280–290, 1999.

[6] N. Alon, V. Rödl. Sharp bounds for some multicolor Ramsey numbers. Combinatorica 25(2):125–141, 2005.

[7] N. Alon, C. Shikhelman. Many T-copies in H-free graphs. Journal of Combinatorial Theory, Series B 121:146–172, 2016.

[8] N. Alon, J.H. Spencer. The Probabilistic Method. Fourth Edition, Wiley, 2016.

[9] L. Babai, A. Gál, A. Widgerson. Superpolynomial lower bounds for monotone span programs. Combinatorica 19(3):301–319, 1999.

[10] L. Babai, A. Gál, J. Kollár, L. Rónyai, T. Szabó, A. Widgerson. Extremal bipartite graphs and superpolynomial lower bounds for monotone span programs. In: G.L. Miller (ed.), Proceedings of STOC'96, ACM, 1996. pp. 603–611.

[11] S. Ball, V. Pepe. Asymptotic Improvements to the Lower Bound of Certain Bipartite Turán Numbers. Combinatorics, Probability and Computing 21:323–329, 2012.

[12] S. Ball, V. Pepe. Forbidden subgraphs in the norm graph. Discrete Mathematics 339(4):1206–1211, 2016.

[13] J. Balogh, W. Samotij. The number of $K_{s,t}$-free graphs. Journal of the London Mathematical Society 83(2):368–388, 2011.

[14] T. Bayer, T. Mészáros, L. Rónyai, T. Szabó, Exploring Projective Norm Graphs, arXiv:1908.05190, 2019.

[15] T. Bayer, T. Mészáros, L. Rónyai, T. Szabó, Exploring projective norm graphs (extended abstract), Acta Mathematica Universitatis Comenianae, Vol. 88(3), 437-441, 2019.

[16] T. Bayer, T. Mészáros, L. Rónyai, T. Szabó, The Automorphism Group of Projective Norm Graphs, preprint, 2021.

[17] C.T. Benson. Minimal regular graphs of girths eight and twelve. Canadian Journal of Mathematics 18:1091–1094, 1966.

[18] P. Blagojević, B. Bukh, R. Karasev. Turán numbers for $K_{s,t}$-free graphs: topological obstructions and algebraic constructions. Israel Journal of Mathematics 197(1):199–214, 2013.

[19] B. Bollobás. Extremal Graph Theory. Academic Press, 1978.

[20] W. Bosma, J. Cannon, C. Playoust. The Magma algebra system I - The user language. Journal of Symbolic Computation **24**:235–265 (1997).

[21] W.G. Brown. On graphs that do not contain a Thomsen graph. Canadian Mathematical Bulletin 9:281–285, 1966.

[22] B. Bukh. Random algebraic construction of extremal graphs. Bullettin of the London Mathematical Society. 47(6):939–945, 2015.

[23] F.R.K Chung, R.L. Graham. Erdős on Graphs. A K Peters, Wellesley, 1998.

[24] F.R.K. Chung, R.L. Graham. Sparse quasi-random graphs. Combinatorica 22:217–244, 2002.

[25] F.R.K. Chung, R.L. Graham, R.M. Wilson. Quasi-random graphs. Combinatorica 9:345–362, 1989.

[26] D. Conlon, J. Fox, Y. Zhao. Extremal results in sparse pseudorandom graphs. Advances in Mathematics 256:206–290, 2014.

[27] Z. Dvir, J. Kollár, S. Lovett. Variety evasive sets. Computational Complexity 23(4):509–529, 2014.

[28] P. Erdős. On sequences of integers no one of which divides the product of two others and related problems. Mitt. Forsch. Institut Mat. und Mech. Tomsk 2:74–82, 1938.

[29] P. Erdős, M. Simonovits. A limit theorem in graph theory. Studia Scientiarum Mathematicarum Hungarica 1:215–235, 1966.

[30] P. Erdős, A.H. Stone. On the structure of linear graphs. Bulletin of the American Mathematical Society 52:1087–1091, 1946.

[31] J. Fox, J. Pach, A. Sheffer, A. Suk, J. Zahl. A semi-algebraic version of Zarankiewicz's problem. Journal of the European Mathematical Society 19(6):1785–1810, 2017.

[32] Z. Füredi. New asymptotics for bipartite Turán numbers. Journal of Combinatorial Theory, Series A 75(1):141–144, 1996.

[33] Z. Füredi. An upper bound on Zarankiewicz'problem. Combinatorics, Probability and Computing 5(1):29–33, 1996.

[34] L. Foster. HT90 and "simplest" number fields. Illinois Journal of Mathematics 55(4):1621–1655, 2011.

[35] B. Gordon, W.H. Mills, L.R. Welch. Some new difference sets. Canadian Journal of Mathematics 14:614–625, 1962.

[36] C. Grosu. A note on projective norm graphs. International Journal of Number Theory 14(1):55-62, 2018.

[37] Y. Kohayakawa, V. Rödl, P. Sissokho. Embedding graphs with bounded degree in sparse pseudorandom graphs. Israel Journal of Mathematics 139(1):93–137, 2004.

[38] J. Kollár, L. Rónyai, T. Szabó. Norm-graphs and bipartite Turán numbers. Combinatorica 16:399–406, 1996.

[39] A. Kostochka, D. Mubayi, J. Verstraëte. Turán problems and shadows III: expansions of graphs. SIAM Journal on Discrete Mathematics 29(2): 868–876, 2015.

[40] A. Kostochka, P. Pudlák, V. Rödl. Some constructive bounds on Ramsey numbers. Journal of Combinatorial Theory, Series B 100:439–445, 2010.

[41] T. Kővári, V. T. Sós, P. Turán. On a problem of K. Zarankiewicz. Colloquium Mathematicae 3(1):55–57, 1954.

[42] M. Krivelevich, B. Sudakov. Pseudo-random Graphs. In: E. Győri, Gy.O.H. Katona, L. Lovász, T. Fleiner (eds.), More Sets, Graphs and Numbers: A Salute to Vera Sós and András Hajnal, Bolyai Society Mathematical Studies 15, Springer-Verlag, Berlin, Heidelberg, 2006. pp. 199–262.

[43] A.G. Kurosh. Higher Algebra. MIR Publishers, 1972.

[44] S. Lang. Algebra. Springer-Verlag, New York, 2002.

[45] F. Lazebnik, D. Mubayi. New lower bounds for Ramsey numbers of graphs and hypergraphs. Advances in Applied Mathematics 28(3):544–559, 2002.

[46] R. Lidl, H. Niederreiter. Finite Fields. Encyclopedia of Mathematics and its Applications. 2nd ed., Cambridge University Press, 1997.

[47] J. Ma. On edges not in monochromatic copies of a fixed bipartite graph. Journal of Combinatorial Theory, Series B 123:240–248, 2017.

[48] W. Mantel. Problem 28. Winkundige Opgaven 10:60–61, 1907.

[49] T. Mészáros, L. Rónyai, T. Szabó, Singer difference sets and the projective norm graph, arXiv:1908.05591, 2019.

[50] E. L. Monte Carmelo, J. Sanches. Multicolored set multipartite Ramsey numbers. Discrete Mathematics 339:2775–2784, 2016.

[51] E.H. Moore, H.S. Pollatsek. Difference sets: Connecting Algebra, Combinatorics, and Geometry. Student Mathematical Library 67, American Mathematical Society, 2013.

[52] C. J. Moreno, O. Moreno, Exponential sums and Goppa codes: I, Proceedings of the American Mathematical Society 111(2):523–531, 1991.

[53] D. Mubayi. Some exact results and new asymptotics for hypergraph Turán numbers. Combinatorics, Probability and Computing 11(3): 299–309, 2002.

[54] D. Mubayi. Coloring with three-colored subgraphs. Journal of Graph Theory 42(3):193–198, 2003.

[55] D. Mubayi, J. Williford. On the independence number of the Erdős-Rényi and projective norm graphs and a related hypergraph. Journal of Graph Theory 56(2):113–127, 2007.

[56] V. Nikiforov. A contribution to the Zarankiewicz problem. Linear Algebra and its Applications 432:1405–1411, 2010.

[57] V. Nikiforov. Some new results in extremal graph theory. In: Robin Chapman (ed.), Surveys in Combinatorics 2011, LMS Lecture Note Series 392, Cambridge University Press, 2011. pp. 141–182.

[58] B. Nica. Unimodular graphs and Eisenstein sums. Journal of Algebraic Combinatorics 45(2):423–454, 2017.

[59] J. Pach, J. Spencer, G. Tóth. New Bounds on Crossing Numbers. Discrete and Computational Geometry 24(4)623–644, 2000.

[60] C. Palmer, M. Tait, C. Timmons, A.Zs. Wagner. Turán numbers for Berge-hypergraphs and related extremal problems. Discrete Mathematics 342(6):1553–1563, 2019.

[61] X. Peng, C. Timmons. Infinite Turán Problems for Bipartite Graphs. SIAM Journal of Discrete Mathematics 28(2):702–710, 2014.

[62] G. Perarnau, B. Reed. Existence of spanning F-free subgraphs with large minimum degree. Combinatorics, Probability and Computing 26(3):448–467, 2017.

[63] A. Pott. Finite Geometry and Character Theory. Lecture Notes in Mathematics 1601, Springer-Verlag, Berlin, Heidelberg, 1995.

[64] J. Rué, O. Serra, L. Vena. Counting configuration-free sets in groups. European Journal of Combinatorics 66:28—307, 2017.

[65] J. Singer. A Theorem in Finite Projective Geometry and Some Applications to Number Theory. Transactions of the America Mathematical Society 43(3):377–385, 1938.

[66] B. Sudakov, J. Verstraëte. Cycle lengths in sparse graphs. Combinatorica. 28(3):357–372, 2008.

[67] B. Sudakov, J. Vondrák. A randomized embedding algorithm for trees. Combinatorica 30(4)445–470, 2010.

[68] T. Szabó. On the spectrum of projective norm-graphs. Information Processing Letters 86(2):71-74, 2003.

[69] A. Thomason. Pseudo-random graphs. Annals of Discrete Mathematics 33:307–331, 1987.

[70] A. Thomason. Random graphs, strongly regular graphs and pseudo-random graphs. In: C. Whitehead (ed.), Surveys in Combinatorics 1987, LMS Lecture Note Series 123, Cambridge University Press, 1987. pp. 173–195.

[71] P. Turán. On an extremal problem in graph theory. Matematikai és Fizikai Lapok 48:436–452, 1941.

[72] J. Verstraëte. Product representations of polynomials. European Journal of Combinatorics 27:1350–1361, 2006.

[73] L.A. Vinh. The sovability of norm, bilinear and quadratic equations over finite fields via spectra of graphs. Forum Mathematicum 26(1):141–175, 2014.

[74] Y. Wang, Y. Li. Bounds for Bipartite Rainbow Ramsey Numbers. Graphs and Combinatorics 33(4):1065–1079, 2017.

[75] X. Wang, Q. Lin. Multicolor bipartite Ramsey numbers of $K_{t,s}$ and large $K_{n,n}$. Discrete Applied Mathematics 213:238–242, 2016.

5 Appendix

5.1 Characters

Next we recall some basic facts about characters of finite fields. For proofs and further results the interested reader may consult e.g. [46, Chapter 5].

For a finite Abelian group G a group homomorphism χ from G to the multiplicative group $\mathbb{C}^*$ of complex numbers is called a *character* of G. The smallest integer $m \in \mathbb{N}$ such that $\chi^m \equiv 1$ is called the *order* of χ.

A particular multiplicative character in a finite cyclic group G is its *quadratic character* η_G. It is defined as

$$\eta_G(a) = \begin{cases} 1 & \text{if } \exists b \in G : b^2 = a \\ -1 & \text{otherwise} \end{cases}.$$

η_G is indeed a character of G and is of order 1 or 2, depending on whether $|G|$ is odd or even.

5.1.1 Multiplicative characters

Let q be a prime power. A character χ of the multiplicative group $\mathbb{F}_q^*$ is called a *multiplicative character* of $\mathbb{F}_q$. Most of the times it is convenient to extend χ to the whole of $\mathbb{F}_q$ by setting $\chi(0) = 0$, and, by slightly abusing notation, we identify χ with this extension. A particular example of a multiplicative character is the quadratic character of $\mathbb{F}_q$.

Theorem 5 (multiplicative Weil-type bound)**.** *[46, Thm 5.41] Let q be a prime power, χ a multiplicative character of $\mathbb{F}_q$ of order $m \geq 1$ and let $f \in \mathbb{F}_q[X]$ be a monic polynomial of positive degree that is not an m^{th} power of a polynomial. Let d be the number of distinct roots of f in its splitting field over $\mathbb{F}_q$. Then for every $a \in \mathbb{F}_q$ we have*

$$\left| \sum_{c \in \mathbb{F}_q} \chi(af(c)) \right| \leq (d-1)\sqrt{q}.$$

If $f = g^m$ for some and $g \in \mathbb{F}_q[X]$, then

$$\sum_{c \in \mathbb{F}_q} \chi(af(c)) = (q-r)\chi(a),$$

where r is the number of distinct roots of g over $\mathbb{F}_q$.

5.1.2 Additive characters

Let $q = p^k$ be a prime power. A character ψ of the additive group of $\mathbb{F}_q$ is called an *additive character* of $\mathbb{F}_q$. A particular example of an additive character is $\psi(x) = (-1)^{\mathrm{Tr}_{k,p}(x)}$.

A rational function $r(X)$ over $\mathbb{F}_q$ is said to be *degenerate* if it is of the form $(h(X))^p - h(X)$ for some rational function $h(X)$ over $\overline{F}_q$.

Theorem 6 (additive Weil-type bound)**.** *[52, Thm 2] Let q be a prime power, ψ a non-trivial additive character of $\mathbb{F}_q$ and $r(X) = \frac{f(x)}{g(x)}$ a non-degenerate rational function over $\mathbb{F}_q$. Then there exists a positive constant $a \in \mathbb{R}$, depending only on the degree of f and g, such that*

$$\left| \sum_{X \in \mathbb{F}_q \setminus S} \psi\left(r(X)\right) \right| \leq a\sqrt{q},$$

where $S \subseteq \mathbb{F}_q$ is the set of poles of r.

5.1.3 Quadratic equations over finite fields

Among others, characters can be used to express the number of roots of a quadratic polynomial over a finite field, as summarized in the following proposition.

Proposition 7. *Let $q = p^k$ a prime power and $b, c \in \mathbb{F}_q$. Then the number of distinct roots in $\mathbb{F}_q$ of the quadratic polynomial $X^2 + bX + c \in \mathbb{F}_q[X]$ is*

(i) $1 + \eta_{\mathbb{F}_q}(b^2 - 4c)$ *when p is odd,*

(ii) and $\begin{cases} 1 & \text{if } b = 0 \\ 1 + (-1)^{\mathrm{Tr}_{k,2}\left(\frac{c}{b^2}\right)} & \text{if } b \neq 0 \end{cases}$, *when $p = 2$.*

5.2 Proof of Theorem 1

Claim 1. *Let $q = 2^k$ and for $(c_1, c_2) \in \left(\mathbb{F}_q^*\right)^2$ let $f(b) = f_{c_1,c_2}(b) = b(b + c_1)^2$ and $g(b) = g_{c_1,c_2}(b) = (b^2 + b(1 + c_1 + c_2) + c_1)^2$. Then the rational function $\frac{f}{g}$ is of the form $\left(\frac{h_1}{h_2}\right)^2 + \frac{h_1}{h_2}$ for some $h_1, h_2 \in \overline{\mathbb{F}}_q[b]$ if and only if $(c_1, c_2) = (1, 1)$ and in this case we have $\mathrm{Tr}_{k,2}\left(\frac{f(b)}{g(b)}\right) = 0$ for every $b \in \mathbb{F}_q,\ g(b) \neq 0$.*

Proof. First note that $\frac{f(b)}{g(b)}$ cannot be simplified further. Indeed as $c_1 \neq 0$ we have that $g(b)$ is not divisible by b, on the other hand as $b^2 + b(1 + c_1 + c_2) + c_1 = (b + c_1)(b + 1 + c_2) + c_1c_2$ and $c_1c_2 \neq 0$, $g(b)$ is not divisible by $b + c_1$ either.

Now suppose that $\frac{f}{g}$ is degenerate, i.e. there are $h_1, h_2 \in \overline{F}_q[b]$ such that

$$\frac{f}{g} = \left(\frac{h_1}{h_2}\right)^2 + \frac{h_1}{h_2} = \frac{h_1^2 + h_1 \cdot h_2}{h_2^2}.$$

Here we can suppose without loss of generality that the right hand side is also reduced, which happens exactly if $\frac{h_1}{h_2}$ is such. However in this case we must have $h_2 = b^2 + b(1 + c_1 + c_2) + c_1$ and $\deg(h_1) \leq 2$. Therefore let $h_1(b) = \alpha b^2 + \beta b + \gamma$ for some $\alpha, \beta, \gamma \in \mathbb{F}_q$. Substituting this above and comparing the coefficients of the different powers of b we arrive at the following system of equations.

$$b^4 :\ 0 = \alpha^2 + \alpha \tag{20}$$
$$b^3 :\ 1 = \beta + \alpha(1 + c_1 + c_2) \tag{21}$$
$$b^2 :\ 0 = \beta^2 + \gamma + \alpha c_1 + \beta(1 + c_1 + c_2) \tag{22}$$
$$b :\ c_1^2 = \beta c_1 + \gamma(1 + c_1 + c_2) \tag{23}$$
$$1 :\ 0 = \gamma^2 + \gamma c_1 \tag{24}$$

Case 1: $1 + c_1 + c_2 = 0$

Then by (21) we have $\beta = 1$ and hence by (23) we deduce that $c_1^2 = c_1$. As $c_1 \neq 0$ this means that $c_1 = 1$, in which case the starting assumption implies $c_2 = 0$ which is impossible.

Case 2: $1 + c_1 + c_2 \neq 0$

By (20) we have $\alpha = 0$ or $\alpha = 1$, and by (24) we have $\gamma = 0$ or $\gamma = c_1$

Case 2a: $\alpha = 0$, $\gamma = 0$

By substituting into (21) we obtain $\beta = 1$. Then, by substituting further into (22) we arrive at $c_1^2 = c_1$. As $c_1 \neq 0$, this in turn implies $c_1 = 1$. Finally, by substituting into (22) we obtain $0 = c_1 + c_2$ and hence $c_2 = 1$.

Case 2b: $\alpha = 0$, $\gamma = c_1$

As in the previous case, (21) again results $\beta = 1$. Then, by substituting into (22) we arrive at $c_2 = 0$, which is impossible.

Case 2c: $\alpha = 1$, $\gamma = 0$

By substituting into (23) we obtain $0 = c_1(c_1 + \beta)$. As $c_1 \neq 0$, this in turn implies $\beta = c_1$. Then, by substituting further into (21) we arrive at $c_2 = 0$, which is impossible.

Case 2d: $\alpha = 1$, $\gamma = c_1$

By substituting into (21) we obtain $\beta = c_1 + c_2$. Then, by substituting further into (22) we arrive at $c_1 = c_2$. Finally, by substituting into (23) we obtain $c_1^2 = c_1$. As $c_1 \neq 0$, this in turn implies $c_1 = c_2 = 1$.

Note that for $(c_1, c_2) = (1, 1)$ the function $\frac{f}{g}$ is degenerate, as witnessed by $h_1(b) = b$ and $h_2(b) = b^2 + b + 1$. □

5.3 Infinite projective norm graphs and difference sets

Projective norm graphs were originally defined only over finite fields, but they extend naturally to a more general setting. For this let $\mathbb{F}$ be an arbitrary field and $t \geq 2$ an integer. Further let $\mathbb{K}_t$ be a cyclic

Galois extension of $\mathbb{F}$ of degree t and let us denote by $\mathrm{N} = \mathrm{N}_{\mathbb{K}/\mathbb{F}}$ and $\mathrm{Tr} = \mathrm{Tr}_{\mathbb{K}/\mathbb{F}}$ the norm and the trace of this extension, respectively. That is, for $A \in \mathbb{K}$ we have $\mathrm{N}(A) = A \cdot \phi(A) \cdot \phi^{(2)}(A) \cdots \phi^{(t-1)}(A)$ and $\mathrm{Tr}(A) = A + \phi(A) + \phi^{(2)}(A) + \cdots + \phi^{(t-1)}(A)$, where ϕ is an automorphism generating the Galois group of $\mathbb{K}/\mathbb{F}$ and $\phi^{(j)}$ denotes the j-fold iteration of ϕ. Then the *projective norm-graph* $\mathrm{NG}(\mathbb{F}, \mathbb{K})$ has vertex set $\mathbb{K} \times \mathbb{F}^*$, and two vertices (A, a) and (B, b) are adjacent if and only if $\mathrm{N}(A+B) = ab$. $\mathrm{NG}(\mathbb{F}, \mathbb{K})$ is the general variant of the $K_{t+1,t!+1}$-free projective norm graph $\mathrm{NG}(q, t+1)$. Because of the generality of the key lemma in [5], the very same proof, without any modifications, also gives that $\mathrm{NG}(\mathbb{F}, \mathbb{K})$ is $K_{t+1,t!+1}$-free.

When studying $\mathrm{NG}(q, 4)$, in our proofs we made great use of the difference sets that arose naturally in connection with the norm equation systems we studied. Many of our results about these difference sets carry over to the general setting of cyclic Galois extensions we just encountered, in which case our main focus of interest will be on the subset

$$\mathcal{S}_t = \{\overline{Y} \mid Y \in \mathbb{K}^*,\ \mathrm{Tr}_{\mathbb{K}/\mathbb{F}}(Y) = 0\}$$

of the multiplicative group ${}^{\mathbb{K}^*}\!/_{\mathbb{F}^*}$, where $\overline{Y}$ denotes the image of $Y \in \mathbb{K}^*$ under the natural map $\mathbb{K}^* \to {}^{\mathbb{K}^*}\!/_{\mathbb{F}^*}$.

Earlier we have already introduced (planar) difference sets. In general an (n, m, λ) difference set is a set $\mathcal{D}$ of m elements in a multiplicative group $\mathcal{G}$ of order n, such that any element $A \in \mathcal{G}$ has exactly λ mixed product representations with respect to $\mathcal{D}$. In the planar setting it was Singer [65] who constructed such structures first, using the finite projective plane $\mathrm{PG}(q, 2)$. Singer's result naturally generalizes to the case with parameters of the form $(n, m, \lambda) = (\frac{q^t-1}{q-1}, \frac{q^{t-1}-1}{q-1}, \frac{q^{t-2}-1}{q-1})$ for any prime power q and $t \geq 3$, which are called Singer parameters. We can recover this general construction by considering the set $\mathcal{S}_t$ with $\mathbb{F} = \mathbb{F}_q$ and $\mathbb{K} = \mathbb{F}_{q^t}$ [63].

For multiplicative groups G_1, G_2 two difference sets $\mathcal{D}_1 \subset G_1$ and $\mathcal{D}_2 \subset G_2$ are called *equivalent* if there exists a group isomorphism $\varphi : G_1 \to G_2$ and an element $\Gamma \in G_2$ such that $\varphi(\mathcal{D}_1) = \Gamma \cdot \mathcal{D}_2$. For example, in Abelian groups any difference set $\mathcal{D}$ is equivalent to its inverse $\mathcal{D}^{-1}$ via the isomorphism $X \to \frac{1}{X}$. In the planar case $t = 3$ it is conjectured that any $(q^2 + q + 1, q + 1, 1)$ difference set is equivalent to Singer's construction. As we will see shortly, out construction from Theorem 3 is also equivalent to it. However, for many values $t > 3$ difference sets having Singer parameters yet being inequivalent to Singer's construction are known to exist (see e.g. [35]).

The difference set structure of $\mathcal{S}_t$ in case of finite fields can be extended for arbitrary $\mathbb{F}$, using the natural $(t-1)$-dimensional projective space structure on ${}^{\mathbb{K}^*}\!/_{\mathbb{F}^*}$ (which is induced by the t-dimensional $\mathbb{F}$-vector space structure of $\mathbb{K}$). It turns out that for any non-identity element $\overline{A}$, the set of $\mathcal{S}_t$-elements from the mixed representations of $\overline{A}$ with respect to $\mathcal{S}_t$ forms a subspace of projective dimension $t-3$.

Proposition 8. *Let $\overline{\mathcal{L}}$ be a subspace of ${}^{\mathbb{K}^*}\!/_{\mathbb{F}^*}$ of projective dimension $t-2$. Then for every element $\overline{A} \in {}^{\mathbb{K}^*}\!/_{\mathbb{F}^*} \setminus \{\overline{1}\}$ the set*

$$\mathcal{R}_{\overline{\mathcal{L}}}\left(\overline{A}\right) = \{\overline{B} \in \overline{\mathcal{L}} \mid \exists\ \overline{C} \in \overline{\mathcal{L}} \text{ such that } \overline{A} = \overline{B}\overline{C}^{-1}\} = \{\overline{B} \in \overline{\mathcal{L}} \mid \overline{B}/\overline{A} \in \overline{\mathcal{L}}\}$$

forms a subspace of projective dimension $t-3$.

Proof. Let $\mathcal{L}$ be a $(t-1)$-dimensional subspace of $\mathbb{K}$ over $\mathbb{F}$ such that $\overline{\mathcal{L}} = {}^{\mathcal{L} \setminus \{0\}}\!/_{\mathbb{F}^*}$. Then for any element $\overline{A} \in {}^{\mathbb{K}^*}\!/_{\mathbb{F}^*} \setminus \{\overline{1}\}$ we have

$$\mathcal{R}_{\overline{\mathcal{L}}}\left(\overline{A}\right) = {}^{\mathcal{R}_{\mathcal{L}}(A) \setminus \{0\}}\!/_{\mathbb{F}^*},$$

where $A \in \mathbb{K}^* \setminus \mathbb{F}^*$ is such that $\overline{A} = A \cdot \mathbb{F}^*$ and

$$\mathcal{R}_{\mathcal{L}}(A) = \{B \in \mathcal{L} \mid \exists\ C \in \mathcal{L} \text{ such that } A = BC^{-1}\}.$$

Observe that $\mathcal{R}_{\mathcal{L}}(A) = \mathcal{L} \cap A\mathcal{L}$, where $A\mathcal{L} = \{AL \mid L \in \mathcal{L}\}$.

Since $A \notin \mathbb{F}^*$, the $(t-1)$-dimensional subspaces $\mathcal{L}$ and $A\mathcal{L}$ are different, hence their intersection has dimension $t-2$. Therefore the projective dimension of $\mathcal{R}_{\overline{\mathcal{L}}}\left(\overline{A}\right)$ is indeed $t-3$. □

Corollary 5. *Let q be a prime power and $\overline{\mathcal{L}}$ be a subspace of $\mathbb{F}_{q^t}^* \big/ \mathbb{F}_q^*$ of projective dimension $t-2$. Then $\overline{\mathcal{L}}$ is a $(\frac{q^t-1}{q-1}, \frac{q^{t-1}-1}{q-1}, \frac{q^{t-2}-1}{q-1})$ difference set in the multiplicative group $\mathbb{F}_{q^t}^* \big/ \mathbb{F}_q^*$. In particular, so is $\mathcal{S}_t$.*

Proof. The set $\mathcal{R}_{\overline{\mathcal{L}}}\left(\overline{A}\right)$ is in a one-to-one correspondence with the collection of mixed $\overline{\mathcal{L}}$-respresentations of $\overline{A}$. Since a projective space of dimension $t-i$ over $\mathbb{F}_q$ has size $\frac{q^{t-i+1}-1}{q-1}$, the parameters of the difference set follow.

Finally note that as $\mathrm{Tr}_{\mathbb{K}/\mathbb{F}} : \mathbb{K} \to \mathbb{F}$ is a non-trivial $\mathbb{F}$-linear function, $\mathrm{Ker}(\mathrm{Tr}_{\mathbb{K}/\mathbb{F}})$ is a $(t-1)$-dimensional subspace of $\mathbb{K}$. Hence the set $\mathcal{S}_t = \mathrm{Ker}(\mathrm{Tr}_{\mathbb{K}/\mathbb{F}}) \setminus \{0\} \big/ \mathbb{F}^*$ is a subspace of $\mathbb{K}^* \big/ \mathbb{F}^*$ of projective dimension $t-2$, and as such is a difference set with Singer parameters. □

In Theorem 3 we described a planar difference set as the root set of a simple polynomial and gave explicit formulas of the product representation of each element. Here we extend this result to the general setting. For this let $\mathcal{N}$ denote the group of elements of norm 1 in $\mathbb{K}$. Furthermore, we shall consider the function

$$d_t(X) = 1 + X + X\phi(X) + X\phi(X)\phi^{(2)}(X) + \cdots + X\phi(X)\cdots\phi^{(t-2)}(X).$$

We remark that the function $d_t(X)$ appears in a paper of Foster [34] in a completely different context, in the formulation of the, so called, 'Murphy condition'.

In the next theorem we show that the set

$$\mathcal{D}_t = \{A \in \mathbb{K} \ : \ d_t(A) = 0\}$$

of roots of $d_t(Y)$ in $\mathbb{K}$ is contained in the multiplicative group $\mathcal{N}$ and has the same difference set property as $\mathcal{S}_t$, namely that the mixed representation of any element $A \in \mathcal{N} \setminus \{1\}$ with respect to $\mathcal{D}_t$ form (in some sense) a projective space of dimension $t-3$ over $\mathbb{F}$. In addition we will also be able to describe concisely these product representations.

Theorem 7. *There is a group isomorphism $\overline{\Phi} : \mathbb{K}^* \big/ \mathbb{F}^* \to \mathcal{N}$ such that $\overline{\Phi}(\mathcal{S}_t) = \mathcal{D}_t$. In particular, through $\overline{\Phi}$, the set $\mathcal{D}_t$ inherits the difference set property of $\mathcal{S}_t$ just like the projective space structure. Moreover, given an element $A \in \mathcal{N} \setminus \{1\}$ the different mixed representations of A with respect to $\mathcal{D}_t$ are exactly the products $B \cdot \left(\frac{B}{A}\right)^{-1}$, where B is a root in $\mathbb{K}$ of the function*

$$f_{t,A}(X) = d_t(X) - \frac{1}{\phi^{(t-1)}(A)} \cdot d_t\left(\frac{X}{A}\right).$$

Proof. Consider the $\mathbb{K}^* \to \mathbb{K}^*$ map Φ defined by $X \to \frac{\phi(X)}{X}$. On the one hand, one readily sees that the map Φ maps $\mathbb{K}^*$ into $\mathcal{N}$. On the other hand, by Hilbert's Theorem 90 [44] we know that for every $A \in \mathcal{N}$ there is an element $Y \in \mathbb{K}^*$ such that $A = \Phi(Y)$, which in turn shows that Φ is surjective. Therefore, as $\mathrm{Ker}(\Phi) = \mathbb{F}^*$, the quotient map $\overline{\Phi} : \mathbb{K}^* \big/ \mathbb{F}^* \to \mathcal{N}$ provides an isomorphism between the respective groups.

Next we show that the image of $\mathcal{S}_t$ under the map $\overline{\Phi}$ is $\mathcal{D}_t$. For this let $Y \in \mathbb{K}^*$. Then, on the one hand, we have

$$d_t(\Phi(Y)) = d_t\left(\frac{\phi(Y)}{Y}\right) = 1 + \sum_{j=0}^{t-2}\prod_{i=0}^{j}\frac{\phi^{(i+1)}(Y)}{\phi^{(i)}(Y)} = 1 + \sum_{j=0}^{t-2}\frac{\phi^{(j+1)}(Y)}{Y} = \frac{1}{Y}\,\mathrm{Tr}_{\mathbb{K}/\mathbb{F}}(Y).$$

Therefore, if $\overline{Y} \in \mathcal{S}_t$, then $\overline{\Phi}\left(\overline{Y}\right) \in \mathcal{D}_t$. Finally, let $A \in \mathcal{D}_t$, i.e. A is a root of d_t. Then $\mathrm{N}_{\mathbb{K}/\mathbb{F}}(A) = 1 + A \cdot \phi(d_t(A)) - d_t(A) = 1$, and hence, again by Hilbert's Theorem 90, there is an element $Y \in \mathbb{K}^*$ such that $A = \Phi(Y)$ and so $A = \overline{\Phi}\left(\overline{Y}\right)$. By the above calculations $\mathrm{Tr}_{\mathbb{K}/\mathbb{F}}(Y) = Y \cdot d_t(\Phi(Y)) = Y \cdot d_t(A) = 0$, meaning that $\overline{Y} \in \mathcal{S}_t$. This concludes the proof of $\overline{\Phi}(\mathcal{S}_t) = \mathcal{D}_t$.

Now let us turn to the second part of the theorem. Given an element $A \in \mathcal{N} \setminus \{1\}$ first take a mixed representation $A = B \cdot C^{-1}$ with $B, C \in \mathcal{D}_t$. Then, in particular, we have $C = \frac{B}{A} \in \mathcal{D}_t$ and hence

$d_t(B) = d_t\left(\frac{B}{A}\right) = 0$. Therefore, we have that B is also a root of the function

$$f_{t,A}(X) = d_t(X) - \frac{1}{\phi^{(t-1)}(A)} \cdot d_t\left(\frac{X}{A}\right).$$

For the other direction suppose that B is a root of $f_{t,A}$. Note that then necessarily $B \neq 0$, as otherwise we would have $0 = f_{t,A}(0) = 1 - \frac{1}{\phi^{(t-1)}(A)}$, which is a contradiction as for $A \in \mathcal{N} \setminus \{1\}$ we have $1 - \frac{1}{\phi^{(t-1)}(A)} \neq 0$. To finish the proof we need to show that $B, \frac{B}{A} \in D_t$, as then the product $B \cdot \left(\frac{B}{A}\right)^{-1}$ is a valid product representation of A with respect to $\mathcal{D}_t$. Using that $N_{\mathbb{K}/\mathbb{F}}(A) = 1$ and $\phi^{(t)} \equiv \mathrm{id}$, we have

$$\begin{aligned}
0 = \phi(0) = \phi(f_{t,A}(B)) &= \phi(d_t(B)) - \frac{1}{\phi^{(t)}(A)} \cdot \phi\left(d_t\left(\frac{B}{A}\right)\right) \\
&= \frac{1}{B} \cdot \left(d_t(B) + \mathrm{N}_{\mathbb{K}/\mathbb{F}}(B) - 1\right) - \frac{1}{A} \cdot \frac{1}{\frac{B}{A}} \cdot \left(d_t\left(\frac{B}{A}\right) + \mathrm{N}_{\mathbb{K}/\mathbb{F}}\left(\frac{B}{A}\right) - 1\right) \\
&= \frac{1}{B}\left(d_t(B) - d_t\left(\frac{B}{A}\right)\right) \implies d_t(B) = d_t\left(\frac{B}{A}\right),
\end{aligned}$$

and hence $0 = f_{t,A}(B) = d_t(B)\left(1 - \frac{1}{\phi^{(t-1)}(A)}\right)$. However, as remarked earlier, for $A \in \mathcal{N} \setminus \{1\}$ we have $1 - \frac{1}{\phi^{(t-1)}(A)} \neq 0$, so this at once implies that $d_t(B) = d_t\left(\frac{B}{A}\right) = 0$, and hence $B, \frac{B}{A} \in D_t$, as required. □

Next we spell out the special case of Theorem 7 when $\mathbb{F} = \mathbb{F}_q$, $\mathbb{K} = \mathbb{F}_{q^t}$ and ϕ is the Frobenius automorphism $X \to X^q$. This is a generalization of Theorem 3 and gives a description of the classic Singer difference set inside $\mathcal{N}$ as the set of roots of a simple polynomial and describes the mixed representations of any element also using the roots of a polynomial.

Corollary 6. *Let $q = p^k$ be a prime power, $t \geq 3$ an integer, and let us define over $\mathbb{F}_q$ the polynomial*

$$d_t(Y) = 1 + Y + Y^{1+q} + Y^{1+q+q^2} + \cdots + Y^{1+q+\cdots+q^{t-2}}$$

of degree $\frac{q^{t-1}-1}{q-1}$. Then the set

$$\mathcal{D}_t = \{A \in \mathbb{F}_{q^t} \mid d_t(A) = 0\}$$

of roots of $d_t(Y)$ forms a $(\frac{q^t-1}{q-1}, \frac{q^{t-1}-1}{q-1}, \frac{q^{t-2}-1}{q-1})$-difference set in the cyclic group $\mathcal{N}$ of norm 1 elements of $\mathbb{F}_{q^t}$, which is equivalent to the Singer difference set $\mathcal{S}_t$. Moreover, given an element $A \in \mathcal{N} \setminus \{1\}$, the $\frac{q^{t-2}-1}{q-1}$ different mixed $\mathcal{D}_t$-representations of A are exactly the products $B \cdot \left(\frac{B}{A}\right)^{-1}$, where B is a root in $\mathbb{F}_{q^t}$ of the degree $\frac{q^{t-2}-1}{q-1}$ polynomial

$$f_{t,A}(X) = d_t(X) - A^{1+q+\cdots+q^{t-2}} \cdot d_t\left(\frac{X}{A}\right)$$

□

In connection with Corollary 6 first note that, in particular, it implies that the polynomials $d_t(X)$ and $f_{t,A}(X)$ always split over $\mathbb{F}_{q^t}$. Also, in the special case $t = 3$, we recover the difference set $\mathcal{H}_1$ from Theorem 3. In this case the polynomial $f_{t,A}$ is linear and its unique root is exactly the element A_1 from Theorem 3.