



Delft University of Technology

Excluding Affine Configurations over a Finite Field

Gijswijt, Dion

DOI

[10.19086/da.91186](https://doi.org/10.19086/da.91186)

Publication date

2023

Document Version

Final published version

Published in

Discrete Analysis

Citation (APA)

Gijswijt, D. (2023). Excluding Affine Configurations over a Finite Field. *Discrete Analysis*, 2023, 1-24.
<https://doi.org/10.19086/da.91186>

Important note

To cite this publication, please use the final published version (if applicable).
Please check the document version above.

Copyright

Other than for strictly personal use, it is not permitted to download, forward or distribute the text or part of it, without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license such as Creative Commons.

Takedown policy

Please contact us and provide details if you believe this document breaches copyrights.
We will remove access to the work immediately and investigate your claim.

Excluding Affine Configurations over a Finite Field

Dion Gijswijt

Received 4 April 2022; Published 18 December 2023

Abstract: Let $a_{i1}x_1 + \cdots + a_{ik}x_k = 0$, $i \in [m]$ be a balanced homogeneous system of linear equations with coefficients a_{ij} from a finite field $\mathbb{F}_q$. We say that a solution $x = (x_1, \dots, x_k)$ with $x_1, \dots, x_k \in \mathbb{F}_q^n$ is *generic* if every homogeneous balanced linear equation satisfied by x is a linear combination of the given equations.

We show that if the given system is *tame*, subsets $S \subseteq \mathbb{F}_q^n$ without generic solutions must have exponentially small density. Here, the system is called tame if for every implied system the number of equations is less than half the number of used variables. Using a subspace sampling argument this also gives a ‘supersaturation result’: there is a constant c such that for $\varepsilon > 0$ sufficiently small, every subset $S \subseteq \mathbb{F}_q^n$ of size at least $q^{(1-\varepsilon)n}$ contains $\Omega(q^{(k-m-\varepsilon c)n})$ solutions as $n \rightarrow \infty$. For $q < 4$ the tameness condition can be left out.

Our main tool is a modification of the slice rank method to leverage the existence of many solutions in order to obtain high rank solutions.

Key words and phrases: additive combinatorics, extremal combinatorics, slice rank, Turán number for matroids, affine configurations

1 Introduction

Let $\mathbb{F}_q$ be a finite field. Consider a balanced homogeneous system of linear equations

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1k}x_k &= 0 \\ &\vdots \\ a_{m1}x_1 + \cdots + a_{mk}x_k &= 0 \end{aligned} \tag{*}$$

with coefficient matrix $A = (a_{ij}) \in \mathbb{F}_q^{m \times k}$ and variable vectors $x_1, \dots, x_k \in \mathbb{F}_q^n$. By *balanced*, we mean that $a_{i1} + \dots + a_{ik} = 0$ for all $i \in [m]$. In other words, the equations give affine dependencies between the k variable vectors. We will always assume that the equations are linearly independent, i.e., $\text{rank}(A) = m$. Note that for any $v \in \mathbb{F}_q^n$ we obtain a trivial solution by setting $x_i = v$ for all $i \in [k]$.

If $x = (x_1, \dots, x_k)$ is a solution to $(\star)$, we say that a set $S \subseteq \mathbb{F}_q^n$ contains the solution x if $x_1, \dots, x_k \in S$. For $n \rightarrow \infty$, we are interested in asymptotic upper bounds on the maximum size of a subset $S \subseteq \mathbb{F}_q^n$ that contains no ‘non-degenerate’ solutions to $(\star)$. In particular, we will be interested in the case that S can be shown to have exponentially small density in $\mathbb{F}_q^n$. In this context there are at least three natural notions of non-degeneracy that have previously been studied. A solution $x = (x_1, \dots, x_k)$ to $(\star)$ is said to be

- (a) *non-trivial* if $x_i \neq x_j$ for some $i, j \in [k]$;
- (b) *a $(\star)$ -shape*¹ if $x_1, \dots, x_k$ are pairwise distinct;
- (c) *generic*² if x only satisfies affine relations $\mu_1 x_1 + \dots + \mu_k x_k = 0$ that are linear combinations of the equations in $(\star)$.

Clearly, every $(\star)$ -shape is a non-trivial solution. Every generic solution is a $(\star)$ -shape, except when an equation of the form $x_{j_1} - x_{j_2} = 0$ is implied by $(\star)$ (in which case no $(\star)$ -shape exists in $\mathbb{F}_q^n$).

The question of how large a set without non-degenerate solutions can be, may be asked more generally for abelian groups instead of $\mathbb{F}_q^n$. Especially for $\mathbb{Z}/n\mathbb{Z}$ (or intervals in $\mathbb{Z}$) this is a central problem in additive number theory which includes famous results like Szemerédi’s theorem on arithmetic progressions [25]. Here we will solely focus on the case that the variables take values in $\mathbb{F}_q^n$. It is worth mentioning that $(\star)$ always has a generic solution in $\mathbb{F}_q^{k-m-1}$. Hence, we have $|S| = o(q^n)$ for any $S \subseteq \mathbb{F}_q^n$ without generic solutions to $(\star)$ as a direct consequence of the multi-dimensional density Hales-Jewett theorem [7].

The system $(\star)$ is called³

- *moderate* if there is a $\delta > 0$ such that $|S| = O(q^{(1-\delta)n})$ for any set $S \subseteq \mathbb{F}_q^n$ that does not contain a $(\star)$ -shape,
- *temperate* if there is a $\delta > 0$ such that $|S| = O(q^{(1-\delta)n})$ for any set $S \subseteq \mathbb{F}_q^n$ that does not contain a generic solution to $(\star)$.

It follows that a temperate system is also moderate, provided the system does not imply an equation of the form $x_{j_1} - x_{j_2} = 0$. In this paper we will show that under certain natural restrictions on $(\star)$, the system $(\star)$ is temperate.

Below, we mention some recent work on finding such exponential bounds for each of the three notions of non-degeneracy. In all cases, the main tool is the slice rank method or a variation thereof.

¹This terminology was introduced in [16].

²This terminology was introduced in [5]

³The notions ‘moderate’ and ‘temperate’ were introduced in [16] and [5], respectively.

Non-trivial solutions Perhaps the simplest and most studied system is the single equation $x_1 - 2x_2 + x_3 = 0$ where the solutions are precisely the 3-term arithmetic progressions. In this case, the notions ‘non-trivial’, ‘ $(\star)$ -shape’ and ‘generic’ coincide (for q odd⁴). A set $S \subseteq \mathbb{F}_3^n$ with no nontrivial 3-term progressions is known as a *cap set*. Based on the ground-breaking result of Croot, Lev, and Pach [4], it was shown in [6] that $|S| \leq 3 \cdot 2.756^n$ for any cap set $S \subseteq \mathbb{F}_3^n$. More generally, the authors show that any set $S \subseteq \mathbb{F}_q^n$ without non-trivial solutions to a given balanced equation $a_1x_1 + a_2x_2 + a_3x_3 = 0$ has exponentially small density in $\mathbb{F}_q^n$. In [14] the proof is adapted to upper bound sets in $(\mathbb{F}_q^2)^n$ without right isosceles triangles.

The method used in [6], was recast by Tao into a more elegant, symmetric form introducing the concept of *slice rank* [27, 26]. Using the slice rank method, it is straightforward to generalize the cap set theorem to general balanced systems (see for example Theorem 1.1 in [22] and also Proposition 4.12 in [1]). To describe the upper bound, let

$$m_{q,n,d} = |\{\alpha \in \{0, 1, \dots, q-1\}^n : \alpha_1 + \dots + \alpha_n \leq d\}|$$

denote the number of monomials in n variables of degree at most $d \in \mathbb{R}_{\geq 0}$ in which each variable has exponent at most $q-1$. Using the fact that for any integer d the number of monomials of degree d is the coefficient of t^d in $(1+t+\dots+t^{q-1})^n$, one obtains the following upper bound.

Lemma 1. *Let $\delta \in (0, 1)$. Then*

$$m_{q,n,\delta(q-1)n} \leq c_{q,\delta}^n,$$

where $c_{q,\delta} = \inf_{0 < t \leq 1} (1+t+\dots+t^{q-1})t^{-\delta(q-1)}$. Moreover, $c_{q,\delta} < q$ for $\delta < \frac{1}{2}$.

The slice rank method then yields the following result.

Theorem 2. *Let $S \subseteq \mathbb{F}_q^n$ have no nontrivial solution to $(\star)$. Then*

$$|S| \leq k \cdot m_{q,n,(q-1)nm/k} \leq k \cdot c_{q,m/k}^n.$$

If $k \geq 2m+1$, we have $c_{q,m/k} < q$.

The factor k in the theorem can be removed by the ‘power trick’ since $S_1 \times S_2$ has no nontrivial solution when the same holds for each $S_i \subseteq \mathbb{F}_q^{n_i}$. The cap set theorem corresponds to the case $(m, k) = (1, 3)$. The theorem implies that if $k \geq 2m+1$, every set $S \subseteq \mathbb{F}_q^n$ without non-trivial solutions to $(\star)$ has exponentially small density. When $k \leq 2m$, the slice rank method breaks down since for $d \geq (q-1)n/2$ we have $m_{q,n,d} \geq \frac{1}{2}q^n$, so the obtained upper bound is trivial.

For $k \geq 4$ and any prime $p \geq k$, it is unknown whether every $S \subseteq \mathbb{F}_p^n$ without non-trivial k -term progressions, i.e., without non-trivial solutions to the system

$$\begin{aligned} x_1 - 2x_2 + x_3 &= 0 \\ &\vdots \\ x_{k-2} - 2x_{k-1} + x_k &= 0 \end{aligned}$$

has exponentially small density for $n \rightarrow \infty$.

⁴If q is even, the problem is not interesting. Indeed, x_1, x_2, x_1 is a ‘nontrivial’ 3-AP for any $x_1 \neq x_2$ and, moreover, no 3-AP x_1, x_2, x_3 exists with x_1, x_2 , and x_3 pairwise distinct.

($\star$)-shapes In the case that ($\star$) consists of the single equation $x_1 + \cdots + x_p = 0$ with coefficients in $\mathbb{F}_p$, where $p \geq 3$ is a prime number, the maximum size of a set $S \subseteq \mathbb{F}_p^n$ without ($\star$)-shape is closely related to the Erdős-Ginzburg-Ziv constant $\mathfrak{s}(\mathbb{F}_p^n)$ for the abelian group $\mathbb{F}_p^n$. The slice rank method does not (for $p \geq 5$) yield solutions with all x_i distinct. However, using a variant called *partition rank*, Naslund [19] showed that $S \subseteq \mathbb{F}_p^n$ has exponentially small density if S does not contain a solution to $x_1 + \cdots + x_p = 0$ with the x_i pairwise distinct. Combining the slice rank method with other techniques, the exponent in the upper bound was further improved in [11, 23].

Mimura and Tokushige were the first to explicitly study moderate systems, in part motivated by analogous results over the integers by Ruzsa [21]. In [15, 16, 17, 18] they showed that several specific systems and families of systems are moderate. Perhaps the simplest example is the case where ($\star$) consists of a single balanced equation in $k \geq 3$ variables. A more general theorem containing these specific examples was proved in [5]. There, it is shown that if the coefficient matrix A has many pairs of linearly dependent columns, the system will be moderate. On the opposite end, it was shown in [22] that for $k \geq 3m$, systems in which all $m \times m$ minors of A are nonzero, are moderate.

Generic solutions It is implicit in [22] that if ($\star$) consists of a single equation, the system is temperate. A more general result is shown in [5]. There, two columns of A are said to be equivalent if they are scalar multiples of one another. It is shown that ($\star$) is temperate if either (i) for each equivalence class the columns sum to zero, or (ii) the number of classes is equal to $m + 1$. If ($\star$) consists of a single equation, then there is only one equivalence class and we are in case (i).

In [12], Geelen and Nelson proved a result in extremal matroid theory that is an analogue of the Erdős-Stone theorem for graphs. The theorem states that for a fixed set N of points in the projective space $\text{PG}(m-1, q)$, the maximum size $\text{ex}_q(N, n)$ of a subset $A \subseteq \text{PG}(n-1, q)$ not containing a copy of N satisfies $\frac{\text{ex}_q(N, n)}{|\text{PG}(n-1, q)|} \rightarrow 1 - q^{1-\chi(N)}$ as $n \rightarrow \infty$, where $\chi(N)$ is the critical number of N .

In the case that N is affine ($\chi(N) = 1$), this only gives an upper bound $o(q^n)$ on the Turán number $\text{ex}_q(N, n)$. However, for the binary case it was shown in [2] that in fact $\text{ex}_2(N, n) = O(2^{\alpha n})$ for some $\alpha < 1$ when N is affine. This is equivalent to the statement that for $q = 2$ the system ($\star$) is always temperate.

Main results

We show that under certain conditions, the system ($\star$) is temperate. Our main result is the following.

Theorem A. *The balanced system ($\star$) is temperate if the coefficient matrix A is tame.*

Here, the matrix A is called *tame* if every system implied by ($\star$) that has m' independent equations, uses at least $2m' + 1$ variables. The precise definition of tameness can be found in Section 3. We note that if ($\star$) implies the equation $x_1 - x_2 = 0$, then without loss of generality, A has the following form:

$$A = \left(\begin{array}{c|ccc} 1 & -1 & 0 & \cdots & 0 \\ 0 & & & & \\ \vdots & & & & \\ 0 & & & & \end{array} \begin{array}{c} B \\ \\ \\ \end{array} \right).$$

Then $(\star)$ is temperate if and only if the system with coefficient matrix B is temperate. Hence, we may assume that $(\star)$ does not imply an equation of the form $x_{j_1} - x_{j_2} = 0$.

The systems that were shown to be moderate or temperate in [5, 15, 16, 17, 22] have tame coefficient matrices. Hence these results are implied by Theorem A (albeit with possibly much worse exponents).

Over the fields $\mathbb{F}_2$ and $\mathbb{F}_3$, the tameness condition is not necessary.

Theorem B. *The balanced system $(\star)$ is temperate if $q \in \{2, 3\}$.*

The number of solutions of affine rank $\leq r$ to $(\star)$ in the space $\mathbb{F}_q^n$ is $O(q^r)$. In particular, the total number of solutions is $O(q^{(k-m)n})$. As part of the proof of Theorem A we show a supersaturation result for solutions of a fixed affine rank. Applied to Theorem A and B, we obtain the following corollary.

Corollary C. *Suppose that the coefficient matrix of $(\star)$ is tame or that $q < 4$. Then there exist $\delta > 0$ and $C > 0$ such that for all positive $\delta' < \delta$ the following holds: if $S \subseteq \mathbb{F}_q^n$ has size $|S| \geq q^{(1-\delta')n}$, then S contains $\Omega(q^{(k-m-C\delta')n})$ solutions to $(\star)$.*

Theorems A and B can also be expressed in terms of excluding affine configurations.

Corollary D. *Let $z_1, \dots, z_k \in \mathbb{F}_q^d$ be distinct. Suppose $q < 4$ or that for every $i \in [k]$ the set $\{z_1, \dots, z_k\}$ is the union of two affinely independent subsets containing z_i . Then every subset $S \subseteq \mathbb{F}_q^n$ containing no affine copy of $(z_1, \dots, z_k)$ has exponentially small density in $\mathbb{F}_q^n$ (as $n \rightarrow \infty$).*

Outline paper and proof

In Section 2, we set up our notation and preliminaries.

In Section 3, we introduce *tame* matrices. We give a good characterization for being tame using the matroid union theorem and show that any tame $m \times k$ matrix can be extended to a tame $m' \times (2m' + 1)$ matrix. This allows us to restrict the proof of Theorem A to the case $k = 2m + 1$. The main result in this section is Proposition 16, which shows that for any solution x of rank r that is not generic ($r < (2m + 1) - m$), there are two disjoint affine bases of $\{x_i : i \in [2m + 1]\}$. This is a crucial part of the proof of Theorem A, and the place where the tameness of A is used.

In Section 4 we show a supersaturation result for solutions of a given affine rank. If for some $\delta > 0$ the condition $|S| \geq q^{(1-\delta)n}$ forces solutions of affine rank $\geq r$, then for $\delta' < \delta$ the condition $|S| \geq q^{(1-\delta')n}$ forces S to have $\Omega(q^{r-c\delta'n})$ solutions of affine rank $\geq r$ (for some constant c). This is used in the proof of Theorem A.

In Section 5 we prove our main theorem: Theorem A. It uses ideas from the slice rank method (in particular the Croot-Lev-Pach lemma), the supersaturation result and Proposition 16. The main idea is to assume for contradiction that $r < (2m + 1) - m$ is the maximum affine rank for which we can force solutions in S . We take the indicator function of the solution set $f : S^k \rightarrow \mathbb{F}_q$ and two suitable disjoint sets $I, J \subseteq [k]$ of size r . Summing f against a suitable random $g : S^{[k] \setminus (I \cup J)} \rightarrow \mathbb{F}_q$, we obtain a function $M(f) : S^I \times S^J \rightarrow \mathbb{F}_p$ that can be interpreted as an $|S|^r \times |S|^r$ matrix. Using the CLP lemma, the rank of $M(f)$ can be shown to be ‘small’. On the other hand, Proposition 16 implies that $M(f)$ is the sum of low rank matrices and an almost diagonal matrix that is ‘large’ by the supersaturation result, resulting in a contradiction.

In Section 6 we prove Theorem B. The proof only uses the cap set theorem and an induction trick to lift it to a multi-dimensional variant.

In Section 7 we briefly discuss the relation with affine configurations of points and show Corollary D. Finally, in Section 8 we conclude with Corollary C and an open problem.

2 Preliminaries and notation

We denote the set of nonnegative integers by $\mathbb{N}$. For any positive integer n , we denote $[n] = \{1, \dots, n\}$. Throughout the paper, q will denote a (fixed) prime power and $\mathbb{F}_q$ denotes the field of order q . By $\mathbb{F}$ we will denote an arbitrary field. For a linear space $\mathbb{F}^n$ we denote by $e_1, \dots, e_n$ the standard basis vectors. We will use the following basic lemma from linear algebra.

Lemma 3. *Let S be a set and let $V \subseteq \mathbb{F}^S$ be a linear subspace of dimension $d \in \mathbb{N}$. Then there is a subset $T \subseteq S$ of size $|T| = d$ such that $f \mapsto f|_T$ is an isomorphism between V and $\mathbb{F}^T$.*

Asymptotic notation

The asymptotic notations $O(\cdot)$, $o(\cdot)$, $\Omega(\cdot)$ used in this paper will always be with respect to the dimension n of the space $\mathbb{F}_q^n$. The notation $g(n) = \Omega(f(n))$ refers to the ‘Knuth big omega notation’ common in computer science. In most cases, the function g is implicit. For instance, by the statement ‘For all $S \subseteq \mathbb{F}_q^n$ with property P we have $|S| = \Omega(g(n))$.’ we mean that there exist a constant $C > 0$ and an integer n_0 such that for all $n \geq n_0$ and every $S \subseteq \mathbb{F}_q^n$ with property P we have $|S| \geq Cg(n)$.

Multivariate polynomials

For $\alpha \in \mathbb{N}^n$ we denote by $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ the monomial in variables $x_1, \dots, x_n$ of degree $|\alpha| := \alpha_1 + \dots + \alpha_n$. More generally, if $\alpha = (\alpha_1, \dots, \alpha_k)$, where $\alpha_1, \dots, \alpha_k \in \mathbb{N}^n$, then we write

$$|\alpha| := |\alpha_1| + \dots + |\alpha_k| = \sum_{i=1}^k \sum_{j=1}^n \alpha_{ij} \quad \text{and} \quad x^\alpha := x_1^{\alpha_1} \cdots x_k^{\alpha_k} = \prod_{i=1}^k \prod_{j=1}^n x_{ij}^{\alpha_{ij}}.$$

Since $x^q = x$ for all $x \in \mathbb{F}_q$, we will restrict our polynomials to only have monomials in which all variables occur with exponent at most $q-1$. We write $\mathbb{F}_q[x_1, \dots, x_n]'$ for the linear space spanned by the monomials x^α , $\alpha \in \{0, 1, \dots, q-1\}^n$. For $d \in \mathbb{R}$ we define $M_{q,n,d} = \{\alpha \in \{0, 1, \dots, q-1\}^n : |\alpha| \leq d\}$ and $m_{q,n,d} = |M_{q,n,d}|$.

The following key lemma is due to Croot, Lev and Pach (see [4]).

Lemma 4 (CLP lemma). *Let $f \in \mathbb{F}_q[x_1, \dots, x_n, y_1, \dots, y_n]'$ have degree at most d . Then the $q^n \times q^n$ -matrix M given by $M_{ab} := f(a, b)$ for all $a, b \in \mathbb{F}_q^n$, has rank at most $2m_{q,n,d/2}$.*

Since we will use similar arguments later, we give the proof here.

Proof. Write $f = \sum_{\alpha, \beta} c_{\alpha\beta} x^\alpha y^\beta$ where the sum is over all $\alpha, \beta \in \{0, \dots, q-1\}^n$ that satisfy $|\alpha| + |\beta| \leq d$, and the $c_{\alpha\beta} \in \mathbb{F}_q$ are constants. Since each term has $|\alpha| \leq d/2$ or $|\beta| \leq d/2$, we can group the terms accordingly (if both $|\alpha|, |\beta| \leq d/2$ we can choose either group) and obtain

$$f(x, y) = \sum_{|\alpha| \leq d/2} x^\alpha f_\alpha(y) + \sum_{|\beta| \leq d/2} y^\beta g_\beta(x)$$

for certain $f_\alpha \in \mathbb{F}_q[y_1, \dots, y_n]'$ and $g_\beta \in \mathbb{F}_q[x_1, \dots, x_n]'$. Each of the terms $x^\alpha f_\alpha(y)$ and $y^\beta g_\beta(x)$ corresponds to a rank 1 matrix (as it is the product of a function of x and a function of y). Hence, M has rank at most $2m_{q,n,d/2}$. $\square$

Balanced linear systems

We will consider systems of linear equations of the form

$$\begin{aligned} a_{11}x_1 + \dots + a_{1k}x_k &= 0 \\ &\vdots \\ a_{m1}x_1 + \dots + a_{mk}x_k &= 0 \end{aligned} \tag{*}$$

where the coefficients a_{ij} are elements of a field $\mathbb{F}$ and $x_1, \dots, x_k \in \mathbb{F}^n$ are variable vectors. We will use the shorthand notation $x = (x_1, \dots, x_k) \in \mathbb{F}^{n \times k}$, $A = (a_{ij}) \in \mathbb{F}^{m \times k}$ and write the system of linear equations as⁵ $Ax^\top = 0$. If $\sum_{j \in [k]} a_{ij} = 0$ for all $i \in [m]$, we say that the matrix A is *row-balanced* and that the system $Ax^\top = 0$ is a *balanced* system.

Matroid terminology

Let $A \in \mathbb{F}^{m \times k}$. For a subset $U \subseteq [k]$, we denote by $r_A(U)$ the rank of the submatrix of A formed by the columns indexed by U . We have $r_A(U) = |U|$ if and only if the columns of A indexed by U are linearly independent. We say that U is a *basis* of A if $|U| = r_A(U) = \text{rank}(A)$. Note that any set $I \subseteq [k]$ with $r_A(I) = |I|$ is a subset of a basis.

The pair $M = ([k], \mathcal{I})$ where $\mathcal{I} = \{I \subseteq [k] : r_A(I) = |I|\}$ is a linear matroid with collection of independent sets $\mathcal{I}$ and rank function r_A . The following proposition follows directly by applying the matroid union theorem to two copies of M (see for instance Corollary 42.1b in [24]). It gives a min-max formula for the maximum size of the union of two sets of linearly independent columns of the matrix A .

Proposition 5. *Let $A \in \mathbb{F}^{m \times k}$. Then*

$$\max\{|I \cup J| : I, J \subseteq [k], r_A(I) = |I|, r_A(J) = |J|\} = \min\{k - |U| + 2r_A(U) : U \subseteq [k]\}.$$

⁵We can think of $x = (x_1, \dots, x_k)$ as an $n \times k$ matrix. Then $Ax^\top = 0$, where we take the usual matrix product and 0 denotes the $m \times k$ zero matrix, corresponds to system (*).

Affine rank and generic solutions

Given vectors $x_1, \dots, x_k \in \mathbb{F}^n$, their *affine rank* $\text{arank}\{x_1, \dots, x_k\}$ is the maximum number of affinely independent vectors in $\{x_1, \dots, x_k\}$. In other words,

$$\text{arank}\{x_1, \dots, x_k\} = \text{rank}(X), \text{ where } X = \begin{pmatrix} 1 & \cdots & 1 \\ x_1 & \cdots & x_k \end{pmatrix} \in \mathbb{F}^{(n+1) \times k}.$$

For $x = (x_1, \dots, x_k)$ we will also denote $\text{arank}(x) = \text{arank}(x_1, \dots, x_k) = \text{arank}\{x_1, \dots, x_k\}$.

Definition 6. For $(x_1, \dots, x_k) \in (\mathbb{F}^n)^k$, let

$$\text{Ann}_{\text{bal}}(x_1, \dots, x_k) = \{(\mu_1, \dots, \mu_k) \in \mathbb{F}_q^k : \mu_1 x_1 + \cdots + \mu_k x_k = 0, \mu_1 + \cdots + \mu_k = 0\}.$$

So the elements of $\text{Ann}_{\text{bal}}(x_1, \dots, x_k)$ correspond to the affine relations between $x_1, \dots, x_k$.

Definition 7. If $x = (x_1, \dots, x_k)$ is a solution to $Ax^\top = 0$, we say that $(x_1, \dots, x_k)$ is a *generic* solution if $\text{Ann}_{\text{bal}}(x_1, \dots, x_k) = \text{rowspan}(A)$.

Lemma 8. Let $\mathbb{F}$ be a field and let $x_1, \dots, x_k \in \mathbb{F}^n$. Then

$$\text{arank}(x_1, \dots, x_k) + \dim(\text{Ann}_{\text{bal}}(x_1, \dots, x_k)) = k.$$

Proof. Let $A \in \mathbb{F}^{(n+1) \times k}$ be the matrix

$$A = \begin{pmatrix} 1 & \cdots & 1 \\ x_1 & \cdots & x_k \end{pmatrix}.$$

For $I \subseteq [k]$ the vectors x_i , $i \in I$ are affinely independent if and only if the columns of A indexed by I are linearly independent. So $\text{rank}(A) = \text{arank}(x_1, \dots, x_k)$. Since $\ker(A) = \text{Ann}_{\text{bal}}(x_1, \dots, x_k)$, the result follows from the rank-nullity theorem. $\square$

Lemma 9. Let $A \in \mathbb{F}^{m \times k}$ be a row-balanced matrix of rank m . Let $x = (x_1, \dots, x_k)$ be a solution to $Ax^\top = 0$. Then $\text{arank}(x_1, \dots, x_k) \leq k - m$. Equality holds if and only if $(x_1, \dots, x_k)$ is a generic solution of $Ax^\top = 0$.

Proof. Since $Ax^\top = 0$, the row space of A is contained in $\text{Ann}_{\text{bal}}(x_1, \dots, x_k)$. Therefore we have $m = \text{rank}(A) \leq \dim(\text{Ann}_{\text{bal}}(x_1, \dots, x_k))$, so it follows from Lemma 8 that

$$\text{arank}(x_1, \dots, x_k) = k - \dim(\text{Ann}_{\text{bal}}(x_1, \dots, x_k)) \leq k - m.$$

Clearly we have equality if and only if the row space of A is equal to $\text{Ann}_{\text{bal}}(x_1, \dots, x_k)$, which is equivalent to x being a generic solution. $\square$

Lemma 10. Let $A \in \mathbb{F}^{m \times k}$ be a balanced matrix of rank m . Then $Ax^\top = 0$ has a generic solution in $\mathbb{F}^{k-m-1}$.

Proof. By permuting the k columns of A , and performing elementary row-operations, we may assume that A is of the form $A = \begin{pmatrix} I & B \end{pmatrix}$. Let $z_{m+1}, \dots, z_k \in \mathbb{F}^{k-m-1}$ be affinely independent (e.g. $z_k = 0$, $z_{m+i} = e_i$ for $i \in [k-m-1]$) and set $z_i = -\sum_{j \in [k-m]} B_{ij} z_j$ for $i \in [m]$. Then $z = (z_1, \dots, z_k)$ is a solution to $Ax^\top = 0$ and $\text{arank}(z) = k - m$. So by Lemma 9, z is a generic solution to $Ax^\top = 0$. $\square$

Lemma 11. *Let $A \in \mathbb{F}^{m \times k}$ be a row-balanced matrix of rank m . Let $x = (x_1, \dots, x_k)$ be a solution to $Ax^\top = 0$ such that $\text{arank}(x) = k - m$. Let $U \subseteq [k]$ have size $|U| = m$. Then*

$$U \text{ is a basis of } A \iff \text{arank}\{x_i : i \in [k] \setminus U\} = k - m.$$

Proof. Let $r = r_A(U)$ be the rank of the submatrix induced by the columns in U . By applying row operations to A (and permuting columns in U) we may assume that this submatrix is equal to

$$\begin{pmatrix} I_r & B \\ 0 & 0 \end{pmatrix}$$

where I_r is the $r \times r$ identity matrix.

If U is a basis of A , then $r = m$ and the system $Ax^\top = 0$ expresses for every $j \in U$ the vector x_j as an affine combination of $\{x_i : i \in [k] \setminus U\}$. So $\text{arank}\{x_i : i \in [k] \setminus U\} = \text{arank}\{x_i : i \in [k]\} = k - m$.

If U is not a basis of A , then $r < m$ and hence the equation $a_{m1}x_1 + \dots + a_{mk}x_k$ gives an affine relation between the vectors in $\{x_i : i \in [k] \setminus U\}$ as $a_{mj} = 0$ for all $j \in U$. So $\text{arank}\{x_j : j \in [k] \setminus U\} < k - m$. $\square$

3 Tame matrices

To show that a system $Ax^\top = 0$ is temperate, we will rely on the slice rank method not only for the system $Ax^\top = 0$ itself, but also for implied systems. For this reason, we want the number of variables in an implied system to be more than twice the number of equations. If this is the case, we say that A is *tame*.

Definition 12. Let $A \in \mathbb{F}^{m \times k}$ be a matrix of rank m . We say that A is *tame* if, by elementary row-operations and column permutations, we cannot bring A into the form $\begin{pmatrix} A' & 0 \\ B & C \end{pmatrix}$ where $A' \in \mathbb{F}^{m' \times k'}$ and $k' \leq 2m'$.

Lemma 13. *Let $A \in \mathbb{F}^{m \times k}$ be a matrix of rank m . Then, the following are equivalent:*

- (i) A is tame.
- (ii) For all $U \subsetneq [k]$ we have $2r_A(U) \geq 2m + 1 - k + |U|$.
- (iii) For all $i \in [k]$ the set $[k] \setminus \{i\}$ contains two disjoint bases of A .

Proof.

(ii) $\Rightarrow$ (i). Assume (ii) holds, and suppose that A is not tame. Using elementary row-operations and permuting columns, we can bring A into the form $\tilde{A} = \begin{pmatrix} A' & 0 \\ B & C \end{pmatrix}$ where $A' \in \mathbb{F}^{m' \times k'}$ with $k' \leq 2m'$. Since r_A is preserved under elementary row-operations, the matrix $\tilde{A}$ also satisfies (ii). However, taking $U = \{k' + 1, \dots, k\}$ we obtain a contradiction. Indeed, since C has rank at most $m - m'$, we have $r_{\tilde{A}}(U) \leq m - m'$ and therefore

$$2r_{\tilde{A}}(U) \leq 2m - 2m' \leq 2m - k' = 2m - k + |U|.$$

(i) $\Rightarrow$ (ii). Suppose that (ii) does not hold and let $U \subsetneq [k]$ be such that $2r_A(U) \leq 2m - k + |U|$. Set $k' = k - |U|$ and $m' = m - r_A(U)$. Then

$$k' = k - |U| \leq 2m - 2r_A(U) = 2m'.$$

By permuting columns of A , we may assume that $U = \{k' + 1, \dots, k\}$. By performing elementary row-operations, we can bring A into the form $\begin{pmatrix} A' & 0 \\ B & C \end{pmatrix}$, where C is a $|U| \times r_A(U)$ matrix. Then A' is an $m' \times k$ matrix with $k' \leq 2m'$.

(ii) $\Rightarrow$ (iii). Let $i \in [k]$. For every $U \subseteq [k] \setminus \{i\}$ we have $2r_A(U) \geq 2m + 1 - k + |U|$, or equivalently,

$$(k - 1) - |U| + 2r_A(U) \geq 2m.$$

By Proposition 5 there exist $I, J \subseteq [k] \setminus \{i\}$ such that $|I \cup J| = 2m$ and $r_A(I) = |I|$ and $r_A(J) = |J|$. Hence, I and J are two disjoint bases of A .

(iii) $\Rightarrow$ (ii). Let $U \subsetneq [k]$ and let $i \in [k] \setminus U$. Let $B, B' \subseteq [k] \setminus \{i\}$ be two disjoint bases. Then

$$|U \cap (B \cup B')| \geq |U| - (k - 1 - |B \cup B'|) = |U| - k + 1 + 2m.$$

It follows that

$$2r_A(U) \geq 2 \max\{|U \cap B|, |U \cap B'|\} \geq |U \cap B| + |U \cap B'| \geq |U| - k + 1 + 2m.$$

□

Remark 14. Note that Lemma 13 gives a good characterization of tame matrices in the following sense: if a matrix is not tame, this can be certified by giving a set $U \subsetneq [k]$ that violates the inequality in (ii), and if a matrix is tame, this can be certified by giving two disjoint bases contained in $[k] \setminus \{i\}$ for every $i \in [k]$ as in (iii). In fact, since finding a maximum size set that is the union of two independent sets can be done in polynomial time by the matroid union algorithm, we can check in polynomial time if a given matrix is tame by checking (iii).

Lemma 15. Let $A \in \mathbb{F}^{(m+1) \times (2m+1)}$ have rank $m + 1$, and let A' be obtained by deleting the last row of A . Suppose that A' is tame. Then, there are bases B_1, B_2 of A such that $B_1 \cup B_2 = [2m + 1]$.

Proof. Let $U \subseteq [2m + 1]$. If $|U| = 2m + 1$, then $r_A(U) = m + 1$. If $|U| = 2\ell + 1$ for some $\ell \in \{0, \dots, m - 1\}$, we have $r_A(U) \geq r_{A'}(U) \geq \ell + 1$ by Lemma 13 since A' is tame. If $|U| = 2\ell + 2$ and $u \in U$, we have $r_A(U) \geq r_A(U \setminus \{u\}) \geq \ell + 1$. So we see that

$$2r_A(U) \geq |U| \quad \text{for all } U \subseteq [2m + 1].$$

It now follows by Proposition 5 that there are $I_1, I_2 \subseteq [2m + 1]$ with $r_A(I_1) = |I_1|$, $r_A(I_2) = |I_2|$, and $|I_1 \cup I_2| = 2m + 1$. Extending for $i = 1, 2$ the set I_i to a basis B_i of A completes the proof. □

The following proposition will be of key importance in the proof of Theorem A.

Proposition 16. *Let $A \in \mathbb{F}^{m \times (2m+1)}$ be a balanced, tame matrix of rank m . Let x be a solution to $Ax^\top = 0$ with $\text{arank}(x) = r \leq m$. Then there exist disjoint subsets $I_1, I_2 \subseteq [2m+1]$ of size r , such that $\text{arank}\{x_i : i \in I_1\} = \text{arank}\{x_i : i \in I_2\} = r$.*

Proof. Let $m' = 2m+1-r \geq m+1$. We can extend A with additional rows to obtain a balanced matrix $A' \in \mathbb{F}^{m' \times (2m+1)}$ of rank m' such that $A'x^\top = 0$ (extend the rows of A to a basis of $\text{Ann}_{\text{bal}}(x)$.) Note that we add $m+1-r \geq 1$ rows in total.

Let A'' be the submatrix of A' consisting of the first $m+1$ rows (so A with one row added). By Lemma 15 there exist subsets $J_1, J_2 \subseteq [2m+1]$ of size $m+1$ such that $J_1 \cup J_2 = [2m+1]$ and $r_{A''}(J_1) = r_{A''}(J_2) = m+1$. Clearly, we then also have: $r_{A'}(J_1) = r_{A'}(J_2) = m+1$. It follows that there are bases B_1 and B_2 of A' such that $B_1 \cup B_2 = [2m+1]$. Since $|B_1| = |B_2| = 2m+1-r$, it follows that $I_1 := [2m+1] \setminus B_1$ and $I_2 := [2m+1] \setminus B_2$ are disjoint sets of size r . By Lemma 11, $\text{arank}\{x_i : i \in I_1\} = r = \text{arank}\{x_i : i \in I_2\}$. $\square$

Extending tame matrices

In this subsection we show the following proposition.

Proposition 17. *Let $A \in \mathbb{F}^{m \times k}$ be tame and row-balanced with $k > 2m+1$. Then A can be extended to a tame, row-balanced matrix $A' \in \mathbb{F}^{m' \times (2m'+1)}$ such that if $x' = (x_1, \dots, x_{k'})$ is a generic solution to $A'(x')^\top = 0$, then $x = (x_1, \dots, x_k)$ is a generic solution to $Ax^\top = 0$.*

Before proving the proposition, we need a number of lemmas.

Lemma 18. *Let $A \in \mathbb{F}^{m \times k}$ be tame. Suppose that $k \geq 2m+2$. Then there exist $i \in [k-1]$ such that for all $\alpha, \beta, \gamma \in \mathbb{F} \setminus \{0\}$ the matrix*

$$A' = \begin{pmatrix} A & 0 \\ \alpha e_i^\top + \beta e_k^\top & \gamma \end{pmatrix} \in \mathbb{F}^{(m+1) \times (k+1)}$$

is tame.

Proof. For $U \subseteq [k-1]$ define $f(U) = 2r_A(U) - 2m - 1 + k - |U|$. Since A is tame, it follows by Lemma 13 that $f(U) \geq 0$ for every $U \subseteq [k-1]$. Let

$$\mathcal{T} = \{U \subseteq [k-1] : f(U) = 0\}.$$

Note that $[k-1] \in \mathcal{T}$ since $r_A([k-1]) \leq m$. So $\mathcal{T}$ is nonempty.

Claim. *Let $U, V \in \mathcal{T}$. Then $U \cup V, U \cap V \in \mathcal{T}$.*

Proof of claim. By the submodularity of r_A we have $f(U \cap V) + f(U \cup V) \leq f(U) + f(V) = 0$. Since $f(U \cap V) \geq 0$ and $f(U \cup V) \geq 0$, we have $f(U \cap V) = f(U \cup V) = 0$. $\blacksquare$

Let $I \subseteq [k-1]$ be the unique inclusionwise minimal subset of $\mathcal{T}$. Since $\emptyset \notin \mathcal{T}$ as $k > 2m+1$, the set I is nonempty. Let $i \in I$. So $i \in U$ for all $U \in \mathcal{T}$. We will show that for this choice of i the matrix A' is tame for all $\alpha, \beta, \gamma \in \mathbb{F} \setminus \{0\}$.

Let $U \subsetneq [k+1]$ be arbitrary. By Lemma 13, it suffices to show that

$$2r_{A'}(U) \geq 2(m+1) + 1 - (k+1) + |U|.$$

Suppose that for some $j \in \{i, k, k+1\}$ we have $j \in U$. If $k+1 \in U$ we choose $j = k+1$. Note that $U \setminus \{j\} \subsetneq [k]$. Since $\alpha, \beta, \gamma \neq 0$, we have $r_{A'}(U) \geq 1 + r_A(U \setminus \{j\})$. Since A is tame, we obtain

$$\begin{aligned} 2r_{A'}(U) &\geq 2 + 2r_A(U \setminus \{j\}) \\ &\geq 2 + 2m + 1 - k + |U \setminus \{j\}| \\ &= 2(m+1) + 1 - (k+1) + |U| \end{aligned}$$

as desired.

Therefore, we may assume that $U \cap \{i, k, k+1\} = \emptyset$. So $U \subseteq [k-1]$ and $U \notin \mathcal{T}$. It follows that $f(U) \geq 1$, and therefore

$$\begin{aligned} 2r_{A'}(U) &\geq 2r_A(U) \\ &\geq 1 + (2m + 1 - k + |U|) \\ &= 2(m+1) + 1 - (k+1) + |U|. \end{aligned}$$

□

Note that if $\mathbb{F} \neq \mathbb{F}_2$, we can choose elements $\alpha, \beta, \gamma \in \mathbb{F} \setminus \{0\}$ such that $\alpha + \beta + \gamma = 0$. Hence, if A is row-balanced, we can take A' to be row-balanced as well. For $\mathbb{F} = \mathbb{F}_2$ this does not work. In fact the row-balanced tame matrix $\begin{bmatrix} 1 & 1 & 1 & 1 \end{bmatrix} \in \mathbb{F}_2^{1 \times 4}$ cannot be extended to a row-balanced tame matrix $A' \in \mathbb{F}_2^{2 \times 5}$. For this reason, we need the following lemma.

Lemma 19. *Let $A \in \mathbb{F}_2^{m \times k}$ be tame. Suppose that $k \geq 2m+2$. Then there exists $i \in [k-1]$ such that the matrix $A'' \in \mathbb{F}_2^{(m+3) \times (k+5)}$ given by*

$$A'' := \begin{pmatrix} A & 0 & 0 & 0 & 0 & 0 \\ e_i^\top + e_k^\top & 1 & 0 & 1 & 0 & 0 \\ e_i^\top & 1 & 1 & 0 & 1 & 0 \\ e_k^\top & 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

is tame.

Note that if A has rank m and is row-balanced, then A'' has rank $m+3$ and is row balanced.

Proof. Let i be as in the conclusion of Lemma 18. So the submatrix

$$A' = \begin{pmatrix} A & 0 \\ e_i^\top + e_k^\top & 1 \end{pmatrix}$$

of A'' induced by the first $k+1$ columns and $m+1$ rows is tame. We will use the shorthand notations $r' = r_{A'}$ and $r'' = r_{A''}$. By Lemma 13 we know that

$$2r'(U) \geq 2(m+1) + 1 - (k+1) + |U| \quad \text{for all } U \subsetneq [k+1].$$

Let $U \subsetneq [k+5]$ be arbitrary. To show that A'' is tame, it suffices to show that

$$2r''(U) \geq 2(m+1) + 1 - (k+1) + |U|$$

since $2(m+3) + 1 - (k+5) = 2(m+1) + 1 - (k+1)$.

By permuting the first $k-1$ columns, we may assume without loss of generality that $i = k-1$. Let $U_1 = U \cap [k-2]$ and $U_2 = U \setminus U_1 = U \cap \{k-1, \dots, k+5\}$. First consider the case that $|U_2| \leq 6$. Note that the submatrix of A'' induced by the last three rows and the last seven columns represent all 7 vectors in $\mathbb{F}_2^3 \setminus \{0\}$. Since any set of $t \leq 6$ vectors in $\mathbb{F}_2^3 \setminus \{0\}$ spans a subspace of dimension at least $t/2$, we see that $r''(U) \geq r'(U_1) + |U_2|/2$. Hence,

$$\begin{aligned} 2r''(U) &\geq 2r'(U_1) + |U_2| \\ &\geq 2(m+1) + 1 - (k+1) + |U_1| + |U_2| \\ &= 2(m+1) + 1 - (k+1) + |U|. \end{aligned}$$

Now consider the remaining case that $|U_2| = 7$. Since $k+4$ and $k+5$ belong to U , we have $r''(U) \geq 2 + r'(U \cap [k+1])$. Since U does not contain $[k+1]$ (as $U \neq [k+5]$), we have

$$\begin{aligned} 2r''(U) &\geq 2r'(U \cap [k+1]) + 4 \\ &\geq 2(m+1) + 1 - (k+1) + |U \cap [k+1]| + 4 \\ &= 2(m+1) + 1 - (k+1) + |U|. \end{aligned}$$

□

We are now ready to prove Proposition 17.

Proof. It suffices to show that A can be extended to a row-balanced, tame $k' \times m'$ matrix A' such that the following two properties hold:

- $k' - 2m' = (k - 2m) - 1$,
- if $x' = (x_1, \dots, x_{k'})$ satisfies $A'(x')^\top = 0$ and $\text{arank}\{x'\} = k' - m'$, then $x = (x_1, \dots, x_k)$ satisfies $Ax^\top = 0$ and $\text{arank}(x) = k - m$.

Indeed, repeating this step $k - 2m - 1$ times results in a $(k - m - 1) \times (2(k - m - 1) + 1)$ matrix with the required properties. Note that we used the characterization of generic solutions from Lemma 9.

Let us first consider the case that $\mathbb{F} \neq \mathbb{F}_2$. Let $\alpha, \beta, \gamma \in \mathbb{F} \setminus \{0\}$ be such that $\alpha + \beta + \gamma = 0$. Let $m' = m + 1$ and $k' = k + 1$. By Lemma 18, there exists $i \in [k-1]$ such that the matrix $A' \in \mathbb{F}^{m' \times k'}$ given by

$$A' = \begin{pmatrix} A & 0 \\ \alpha e_i + \beta e_k & \gamma \end{pmatrix}$$

is tame. Since $\alpha + \beta + \gamma = 0$, the matrix A' is balanced. Now suppose $x' = (x_1, \dots, x_{k+1})$ satisfies $A'(x')^\top = 0$ and $\text{arank}(x') = (k+1) - (m+1)$. Let $x = (x_1, \dots, x_k)$. Clearly, $Ax^\top = 0$. Since $\gamma \neq 0$, the vector x_{k+1} is an affine combination of $x_1, \dots, x_k$, so $\text{arank}(x_1, \dots, x_k) = \text{arank}(x_1, \dots, x_{k+1}) = k - m$ as required.

Now let us consider the case that $\mathbb{F} = \mathbb{F}_2$. By Lemma 19, we obtain the tame, row-balanced matrix $A' \in \mathbb{F}_2^{m' \times k'}$ with $m' = m + 3$ and $k' = k + 5$ given by

$$A' := \begin{pmatrix} A & 0 & 0 & 0 & 0 & 0 \\ e_i + e_k & 1 & 0 & 1 & 0 & 0 \\ e_i & 1 & 1 & 0 & 1 & 0 \\ e_k & 1 & 1 & 0 & 0 & 1 \end{pmatrix},$$

where $i \in [k - 1]$. Let $x' = (x_1, \dots, x_{k'})$ satisfy $A'(x')^\top = 0$ and $\text{arank}(x') = k' - m'$. Let $x = (x_1, \dots, x_k)$. Clearly, we have $Ax^\top = 0$. Since x_{k+3} , x_{k+4} and x_{k+5} are affinely dependent on $x_1, \dots, x_{k+2}$, we have $\text{arank}(x') \leq \text{arank}(x_1, \dots, x_{k+2}) \leq \text{arank}(x) + 2$. We obtain

$$\text{arank}(x) \geq \text{arank}(x') - 2 = (k + 5) - (m + 3) - 2 = k - m.$$

Note that by Lemma 9 we also have $\text{arank}(x) \leq k - m$, so we have $\text{arank}(x) = k - m$ as required. $\square$

4 supersaturation

In this section we prove a supersaturation result (Proposition 22) that is essential to the proof of our main theorem. The proof is based on a standard subspace sampling argument (see for instance Exercise 10.1.9 of [28] or [10]). We begin by stating some preliminaries.

For $d, n \in \mathbb{N}$ the *Gaussian binomial coefficient* $\begin{bmatrix} n \\ d \end{bmatrix}_q$ is given by

$$\begin{bmatrix} n \\ d \end{bmatrix}_q = \begin{cases} \prod_{i=0}^{d-1} \frac{1 - q^{n-i}}{1 - q^{d-i}} & \text{if } d \leq n \\ 0 & \text{if } d > n \end{cases}.$$

The following fact is well-known.

Lemma 20. *Let $k \leq d \leq n$ be nonnegative integers. Then the number of d -dimensional linear subspaces of $\mathbb{F}_q^n$ containing a given k -dimensional linear subspace is $\begin{bmatrix} n-k \\ d-k \end{bmatrix}_q$.*

Proof. Let $V \subseteq \mathbb{F}_q^n$ be a k -dimensional linear subspace and let $b_1, \dots, b_k$ be a basis of V . The number of $d - k$ -tuples $(b_{k+1}, \dots, b_d)$ such that $b_1, \dots, b_d$ are linearly independent vectors in $\mathbb{F}_q^n$, is equal to $(q^n - q^k)(q^n - q^{k+1}) \dots (q^n - q^{d-1})$. Indeed, for $i = k + 1, \dots, d$ we can choose b_i arbitrarily in $\mathbb{F}_q^n \setminus \text{span}(b_1, \dots, b_{i-1})$. Thus, we obtain a d -dimensional subspace $W := \text{span}(b_1, \dots, b_d)$ containing V .

Each subspace $W \supseteq V$ of dimension d is thus obtained $(q^d - q^k) \dots (q^d - q^{d-1})$ times, since there are that many ways to extend $b_1, \dots, b_k$ to a basis $b_1, \dots, b_d$ of W . We conclude that the number of d -dimensional subspaces containing V is equal to

$$\frac{(q^n - q^k) \dots (q^n - q^{d-1})}{(q^d - q^k) \dots (q^d - q^{d-1})} = \begin{bmatrix} n-k \\ d-k \end{bmatrix}_q.$$

$\square$

Note that Lemma 20 implies that the number of d -dimensional affine subspaces of $\mathbb{F}_q^n$ that contain a given subset $S \subseteq \mathbb{F}_q^n$ of affine rank r , is equal to $\begin{bmatrix} n-r+1 \\ d-r+1 \end{bmatrix}_q$. Indeed, by shifting, we may assume that $0 \in S$ and then $\dim \text{span}(S) = r - 1$.

We will need the following bounds on the Gaussian binomial coefficients.

Lemma 21. *Let $d \leq n$ be nonnegative integers. Then*

$$q^{d(n-d)} \leq \begin{bmatrix} n \\ d \end{bmatrix}_q \leq 4q^{d(n-d)}.$$

Proof. The lower bound follows directly from the fact that for all $i \in \{0, \dots, d-1\}$ we have

$$\frac{q^{n-i} - 1}{q^{d-i} - 1} \geq \frac{q^{n-i}}{q^{d-i}} = q^{n-d}.$$

The upper bound follows from the fact that for all $i \in \{0, \dots, d-1\}$ we have

$$\frac{q^{n-i} - 1}{q^{d-i} - 1} \leq q^{n-d} \left(1 + \frac{1}{q^{d-i} - 1}\right) \leq q^{n-d} \left(1 + \frac{1}{2^{d-i} - 1}\right)$$

and the fact that

$$\prod_{i=0}^{d-1} \left(1 + \frac{1}{2^{d-i} - 1}\right) = 2 \prod_{i=2}^d \left(1 + \frac{1}{2^i - 1}\right) \leq 2e^{\sum_{i=2}^d \frac{1}{2^i - 1}} \leq 2e^{\frac{1}{3} \sum_{i=0}^{d-2} \frac{1}{2^i}} \leq 2e^{\frac{2}{3}} \leq 4.$$

□

Proposition 22. *Let $A \in \mathbb{F}_q^{m \times k}$ be a row-balanced matrix of rank m . Let r be a positive integer and let $\delta \in (0, 1]$. Suppose that for all $n \geq n_0$ and all $S \subseteq \mathbb{F}_q^n$ of cardinality $|S| \geq q^{(1-\delta)n}$ the set S contains a solution to $Ax^\top = 0$ of affine rank $\geq r$.*

Let $\delta' \in (0, \delta)$. Define

$$n_1 = \lceil \max\left(\frac{\delta}{\delta'} n_0, \frac{2+\delta}{\delta-\delta'}\right) \rceil, \quad \varepsilon = \delta' \cdot \frac{r-1+2\delta}{\delta}, \quad C = \frac{q^2 - 2}{4q^2} q^{-\frac{(r-1+\delta)(2+\delta)}{\delta}}.$$

Then for every $n \geq n_1$ and $S \subseteq \mathbb{F}_q^n$ of size $|S| \geq q^{(1-\delta')n}$, the set S contains at least $Cq^{r n - \varepsilon n}$ solutions to $Ax^\top = 0$ of affine rank at least r .

Proof. Let $N = \lceil \frac{n\delta'+2}{\delta} \rceil$. Note that $N \leq n$ by definition of n_1 . Let $S \subseteq \mathbb{F}_q^n$ have cardinality $|S| \geq q^{(1-\delta')n}$. Let us call an N -dimensional affine subspace V of $\mathbb{F}_q^n$ *rich* if $|V \cap S| > 2q^{(1-\delta)N}$. If V is rich, then $S \cap V$ contains a solution of affine rank at least r since $N \geq n_0$. In fact, since $(S \setminus T) \cap V \geq q^{(1-\delta)N}$ for every set T of size at most $\lceil q^{(1-\delta)N} - 1 \rceil$, the set $S \cap V$ must contain at least $\lceil q^{(1-\delta)N} \rceil$ solutions of rank at least r .

Consider the partition of $\mathbb{F}_q^n$ into the q^{n-N} cosets of a given N -dimensional linear subspace. Let P be the proportion of cosets that are rich. Then

$$Pq^{n-N}q^N + (1-P)q^{n-N}2q^{(1-\delta)N} \geq |S| \geq q^{(1-\delta')n}.$$

Rearranging and dividing by q^n gives

$$P \geq \frac{q^{-\delta'n} - 2q^{-\delta N}}{1 - 2q^{-\delta N}}.$$

Since $\delta N \geq \delta'n + 2$, it follows that

$$P \geq \frac{q^2 - 2}{q^2} q^{-\delta'n}.$$

Let M be the number of pairs (V, x) where $V \subseteq \mathbb{F}_q^n$ is rich and $x = (x_1, \dots, x_k)$ is a solution of affine rank at least r with $x_1, \dots, x_k \in V \cap S$. Then

$$M \geq P \cdot q^{n-N} \begin{bmatrix} n \\ N \end{bmatrix}_q \cdot q^{(1-\delta)N},$$

since there are $P \cdot q^{n-N} \begin{bmatrix} n \\ N \end{bmatrix}_q$ rich subspaces V and for each such V there are at least $q^{(1-\delta)N}$ solutions in $V \cap S$ of rank at least r . Conversely, every solution of affine rank at least r is contained in at most $\begin{bmatrix} n-r+1 \\ N-r+1 \end{bmatrix}_q$ rich affine subspaces V . We conclude that the number of solutions of affine rank at least r in S is at least

$$\begin{aligned} \frac{P \cdot q^{n-N} \cdot q^{(1-\delta)N} \begin{bmatrix} n \\ N \end{bmatrix}_q}{\begin{bmatrix} n-r+1 \\ N-r+1 \end{bmatrix}_q} &\geq \frac{1}{4} P \cdot q^{rn-N(r-1+\delta)} \\ &\geq \frac{q^2 - 2}{4q^2} q^{n(r-\delta')-N(r-1+\delta)} \\ &\geq \frac{q^2 - 2}{4q^2} q^{-(r-1+\delta)\frac{1+\delta}{\delta}} \cdot q^{n(r-\delta')-n\frac{\delta'}{\delta}(r-1+\delta)} \\ &= Cq^{nr-\varepsilon n}, \end{aligned}$$

where we used Lemma 21, the lower bound on P , and the fact that $N \leq \frac{\delta'n}{\delta} + \frac{2+\delta}{\delta}$ in the three inequalities, respectively. $\square$

Remark 23. The obtained value of ε is in general not optimal. In the ‘cap set case’ (i.e. the system is $x_1 - 2x_2 + x_3 = 0$ and $r = 2$), we can take $\delta = 1 - \log_3(2.7552)$ and obtain $\varepsilon = (2 + 1/\delta)\delta' \approx 14.9\delta'$. However, using the bound on the arithmetic triangle removal proved in [8], one can show that we can take $\varepsilon = (1 + 1/\delta)\delta' \approx 13.9\delta'$ as was shown in [20].

5 Proof of Theorem A

In this section, we will prove Theorem A. By Proposition 17, we may restrict ourselves to the case $k = 2m + 1$:

Theorem 24. *Let $A \in \mathbb{F}_q^{m \times (2m+1)}$ be a tame, row-balanced matrix. Then the system $Ax^\top = 0$ is temperate.*

We will need the following lemma.

Lemma 25. *Let M be an $n \times n$ matrix with N nonzero elements such that every row and every column has at most k nonzero elements. Then $\text{rank}(M) \geq \frac{N}{k^2}$.*

Proof. Let $I \subseteq [n]$ be a maximal set of linearly independent columns of M . Let J be the set of rows j for which there is a column $i \in I$ with $M_{ij} \neq 0$. Then $|J| \leq k|I|$ and the support of M must be contained in the rows indexed by J by maximality of I . On the other hand, the rows in J together contain at most $k|J| \leq k^2|I|$ nonzero entries. So $N \leq k^2|I|$. $\square$

The remainder of this section is devoted to proving Theorem 24. It suffices to show the following for all $r \in [m+1]$:

P(r) : There exists a $\delta_r > 0$ such that for all sufficiently large n , every subset $S \subseteq \mathbb{F}_q^n$ with $|S| \geq q^{(1-\delta_r)n}$ contains a solution x to $Ax^T = 0$ with $\text{arank}(x) \geq r$.

The proof is by induction on r . The base case $r = 1$ is trivial since for any $v \in S$ a solution of affine rank 1 is given by $x = (v, \dots, v)$. Hence, we can take $\delta_1 = 1$.

Now let $r \leq m$ and assume that **P(r)** is true. We show that **P($r+1$)** is true. Let $d = n(q-1)\frac{m}{2m+1}$. By Theorem 2, there is an $\varepsilon \in (0, 1)$ such that $m_{q,n,d} = o(q^{(1-\varepsilon)n})$ and $m_{q,rn,d} = o(q^{rn-\varepsilon n})$.

By Proposition 22, there is a $\delta_{r+1} \in (0, \delta_r)$ such that every subset $S \subseteq \mathbb{F}_q^n$ with $|S| \geq q^{(1-\delta_{r+1})n}$ contains $\Omega(q^{rn-\varepsilon n})$ solutions to $Ax^T = 0$ of affine rank at least r . We take δ_{r+1} such that moreover $\delta_{r+1} \leq \varepsilon$.

Now suppose, for the sake of contradiction, that for infinitely many n there is a subset $S \subseteq \mathbb{F}_q^n$ of size $|S| \geq q^{(1-\delta_{r+1})n}$ such that S contains no solution to $Ax^T = 0$ of affine rank at least $r+1$. Consider such pairs (n, S) .

Let $T = \{x \in S^{2m+1} : Ax^T = 0\}$ be the set of all solutions in S . By assumption, every $x \in T$ has affine rank at most r . Let $T_1 := \{x \in T : \text{arank}(x) = r\}$. We have $|T_1| = \Omega(q^{rn-\varepsilon n})$ by our choice of ε . For every $x \in T_1$ there exist, by Proposition 16, disjoint sets $I, J \subseteq [2m+1]$ of size $|I| = |J| = r$ such that $\text{arank}\{x_i : i \in I\} = \text{arank}\{x_i : i \in J\} = r$. Since there are no more than $\binom{2m+1}{r} \binom{2m+1-r}{r}$ possibilities for (I, J) , we may assume without loss of generality that

$$T_2 := \{x \in T_1 : \text{arank}\{x_1, \dots, x_r\} = \text{arank}\{x_{r+1}, \dots, x_{2r}\} = r\}$$

has size $|T_2| \geq \binom{2m+1}{r}^{-1} \binom{2m+1-r}{r}^{-1} |T_1| = \Omega(q^{rn-\varepsilon n})$.

To emphasise the partition $[2m+1] = \{1, \dots, r\} \cup \{r+1, \dots, 2r\} \cup \{2r+1, \dots, 2m+1\}$ of the variables and to simplify notation, we will define $t := 2m+1-2r$ and denote elements from S^{2m+1} by 3-tuples (x, y, z) , where $x, y \in S^r$ and $z \in S^t$.

We will construct a random linear map from $\mathbb{F}_q^{S^{2m+1}}$ to $\mathbb{F}_q^{S^r} \times \mathbb{F}_q^{S^r}$ and interpret the elements of $\mathbb{F}_q^{S^r} \times \mathbb{F}_q^{S^r}$ as $|S|^r \times |S|^r$ matrices. We will give an upper bound on the rank of the resulting matrix that is lower than the expected rank for large n , thus yielding a contradiction.

Recall that $d = n(q-1)\frac{m}{2m+1}$. Let

$$V = \{g : S \rightarrow \mathbb{F}_q : \sum_{z \in S} g(z)z^\alpha = 0 \quad \forall \alpha \in M_{q,n,d}\}.$$

Since $|S| \geq q^{(1-\delta_{r+1})n} \geq q^{(1-\varepsilon)n}$ and $m_{q,n,d} = o(q^{(1-\varepsilon)n})$, we have $\dim(V) \geq |S| - m_{q,n,d} > 0$ (for n large enough). By Lemma 3, there is a subset $S' \subseteq S$ of size $|S'| = \dim(V)$ such that every $h : S' \rightarrow \mathbb{F}_q$ extends

to a unique $g \in V$. Let $W = V^{\otimes t} \subseteq \{g : S^t \rightarrow \mathbb{F}_q\}$ be the linear span of the functions $z \mapsto g_1(z_1) \cdots g_t(z_t)$, where $g_1, \dots, g_t \in V$. Then for every $g \in W$

$$\sum_{z \in S^t} g(z) z_1^{\alpha_1} \cdots z_t^{\alpha_t} = 0 \text{ if } |\alpha_i| \leq d \text{ for some } i \in [t] \quad (1)$$

and every $h : (S')^t \rightarrow \mathbb{F}_q$ extends to a unique $g \in W$.

We choose $h : (S')^t \rightarrow \mathbb{F}_q$ uniformly at random and let $g \in W$ be the extension of h . For any $f : S^{2m+1} \rightarrow \mathbb{F}_q$ we define the random $S^r \times S^r$ matrix $M(f)$ as follows:

$$M(f)_{x,y} := \sum_{z \in S^t} f(x, y, z) g(z).$$

For any subset $X \subseteq S^{2m+1}$ we denote by $\mathbf{1}_X : S^{2m+1} \rightarrow \mathbb{F}_q$ the 0–1 characteristic function of X .

Claim. *The matrix $M(\mathbf{1}_T)$ has rank at most $2m_{q, rn, rd}$.*

Proof of claim. We can write

$$\mathbf{1}_T(x, y, z) = \prod_{i=1}^m \prod_{\ell=1}^n \left[1 - \left(\sum_{j=1}^r a_{i,j} x_{j,\ell} + \sum_{j=1}^r a_{i,j+r} y_{j,\ell} + \sum_{j=1}^t a_{i,j+2r} z_{j,\ell} \right)^{q-1} \right].$$

So $\mathbf{1}_T$ is given by a polynomial of degree at most $mn(q-1)$. Expanding the polynomial, we get

$$\mathbf{1}_T(x, y, z) = \sum_{(\alpha, \beta, \gamma) \in L} c_{\alpha\beta\gamma} x^\alpha y^\beta z^\gamma$$

where $L := \{\ell \in \{0, 1, \dots, q-1\}^{[n] \times [2m+1]} : |\ell| \leq mn(q-1)\}$, and the $c_{\alpha\beta\gamma} \in \mathbb{F}_q$ are certain coefficients. Thus, we have

$$M(\mathbf{1}_T)_{x,y} = \sum_{\alpha, \beta} c'_{\alpha, \beta} x^\alpha y^\beta,$$

where

$$c'_{\alpha, \beta} = \sum_{\gamma: (\alpha, \beta, \gamma) \in L} c_{\alpha, \beta, \gamma} \sum_{z \in S} g(z) z^\gamma.$$

If $|\gamma| \leq td$, then $|\gamma_i| \leq d$ for some $i \in [t]$, and hence $\sum_{z \in S} g(z) z^\gamma = 0$ by definition of g . It follows that $c'_{\alpha, \beta} = 0$ if $|\alpha| + |\beta| \geq mn(q-1) - td = 2rd$. So $M(\mathbf{1}_T)$ is given by a polynomial of degree at most $2rd$ in the rn variables x_{ji} and the rn variables y_{ji} (where $(j, i) \in [r] \times [n]$). Hence, it follows from the CLP lemma that $M(\mathbf{1}_T)$ has rank at most $2m_{q, rn, rd}$. $\blacksquare$

We will now show the following claim.

Claim. *The matrix $M(\mathbf{1}_T)$ has expected rank $\Omega(q^{rn-\varepsilon n})$.*

Proof of claim. Let $T_3 = \{(x, y, z) \in T_2 : z \in (S')^t\}$. For any fixed $b \in \mathbb{F}_q^n$ and any $i \in [t]$ we have $|\{(x, y, z) \in T_2 : z_i = b\}| = O(q^{(r-1)n})$. Since $|S \setminus S'| \leq m_{q, n, d} = o(q^{(1-\varepsilon)n})$, it follows that

$$|T_2 \setminus T_3| = o(q^{rn-\varepsilon n}), \quad |T_3| = \Omega(q^{rn-\varepsilon n}). \quad (2)$$

Let $R = \{(x, y) \in S^r \times S^r : \exists z \in S^t, (x, y, z) \in T_3\}$. Since for each pair (x, y) there are at most q^{rt} possibilities for z (as each z_i is in the affine span of $\{x_i : i \in [r]\}$), it follows that $|R| \geq \frac{|T_3|}{q^{rt}} = \Omega(q^{rn-\varepsilon n})$. Let $(x, y) \in R$. Then

$$M(\mathbf{1}_{T_3})_{x,y} = \sum_{z \in S^t} \mathbf{1}_{T_3}(x, y, z) g(z) = \sum_{z \in (S')^t : (x,y,z) \in T_3} h(z).$$

Since h was chosen uniformly at random and $\{z \in (S')^t : (x, y, z) \in T_3\}$ is nonempty, this sum is nonzero with probability $\frac{q-1}{q}$. So the expected size of the support of $M(\mathbf{1}_{T_3})$ is $\frac{q-1}{q}|R|$.

For every x , there are at most $q^{r(r-1)}$ values of y for which $(x, y) \in R$ since $y_1, \dots, y_r$ are in the affine hull of $x_1, \dots, x_r$. Conversely, for every y there are at most $q^{r(r-1)}$ values of x for which $(x, y) \in R$. So by Lemma 25 we have

$$\text{rank} M(\mathbf{1}_{T_3}) \geq \frac{q-1}{q}|R|/(q^{2r(r-1)}) = \Omega(q^{rn-\varepsilon n}). \quad (3)$$

Recall that for any $(x, y, z) \in T \setminus T_2$ we have $\text{arank}(x) \leq r-1$ or $\text{arank}(y) \leq r-1$. Hence, the number of possibilities for x (resp. y) is $O(q^{(r-1)n})$ and therefore

$$\text{rank} M(\mathbf{1}_{T \setminus T_2}) = O(q^{(r-1)n}). \quad (4)$$

Using the fact that $\text{rank} M(\mathbf{1}_{T_2 \setminus T_3}) \leq |T_2 \setminus T_3| = o(q^{rn-\varepsilon n})$, we conclude that

$$\text{rank} M(\mathbf{1}_T) \geq \text{rank} M(\mathbf{1}_{T_3}) - \text{rank} M(\mathbf{1}_{T_2 \setminus T_3}) - \text{rank} M(\mathbf{1}_{T \setminus T_2}) = \Omega(q^{rn-\varepsilon n}).$$

■

Since $m_{q,rn,rd} = o(q^{rn-\varepsilon n})$, the two claims yield a contradiction for large enough n . This concludes the proof of Theorem 24.

Remark 26. In the proof, we took $r = 1$ as the base case. However the case $r = 2$ also follows directly from Theorem 2, so we could have taken $r = 2$ as a base case as well.

6 Proof of Theorem B

In this section we consider the special case that the finite field is $\mathbb{F}_q$, where $q \in \{2, 3\}$. It turns out that in this case, every balanced system is temperate, by a much simpler argument. The case $q = 2$ is implicit in [2, Lemma 21] in the context of extremal matroid theory.

If $b_0, b_1, \dots, b_d \in \mathbb{F}_q^n$ and $b_1, \dots, b_d$ are linearly independent, then $V = \{b_0 + \alpha_1 b_1 + \dots + \alpha_d b_d : \alpha_1, \dots, \alpha_d \in \mathbb{F}_q\}$ is a d -dimensional affine subspace of $\mathbb{F}_q^n$. A 1-dimensional subspace is also called a *line*.

The main ingredient of the proof of Theorem B is the following lemma.

Lemma 27. *Fix $q \in \{2, 3\}$. Let $d \in \mathbb{Z}_{\geq 1}$. Then there exist $n_d \in \mathbb{Z}_{\geq 1}$, $C_d > 0$ and $\delta_d \in (0, 1]$ such that for all $n \geq n_d$, every $S \subseteq \mathbb{F}_q^n$ of size $|S| \geq C_d q^{(1-\delta_d)n}$ contains an affine d -dimensional subspace.*

The case $q = 3$, the *multidimensional cap set problem*, was proved in [9] by using the arithmetic triangle removal lemma from [8]. A more direct proof (but with slightly worse bounds) due to Jop Briët [3] (personal communication) is given below.

Proof. If $q = 3$, we can take $n_1 = 1$, $C_1 = 3$, and $\delta_1 = 1 - \log_3(2.756)$ by the cap set theorem. If $q = 2$, we can take $n_1 = 1$, $C_1 = 2$, and $\delta_1 = 1$.

Now let $t \geq 2$ and suppose that the statement is true for $d = 1, \dots, t-1$. We define

$$C_t := q(C_1 + C_{t-1}), \quad \delta_t := \frac{\delta_1 \delta_{t-1}}{2 + \delta_1 + \delta_{t-1}}, \quad n_t := \left\lceil \max \left(\frac{2 + \delta_1 + \delta_{t-1}}{\delta_{t-1}} n_1, \frac{2 + \delta_1 + \delta_{t-1}}{2 + \delta_1} n_{t-1} \right) \right\rceil.$$

Note that $0 < \delta_t \leq 1$. Let $n \geq n_t$ and let $S \subseteq \mathbb{F}_q^n$ have size $|S| \geq C_t q^{(1-\delta_t)n}$. We define

$$m = \left\lfloor \frac{\delta_{t-1}}{2 + \delta_1 + \delta_{t-1}} n \right\rfloor, \quad k = \left\lceil \frac{2 + \delta_1}{2 + \delta_1 + \delta_{t-1}} n \right\rceil = n - m.$$

By the choice of n_t we have $m \geq n_1$ and $k \geq n_{t-1}$. For any $x \in \mathbb{F}_q^k$ we denote $S_x := \{y \in \mathbb{F}_q^m : (x, y) \in S\}$. Let $T = \{x \in \mathbb{F}_q^k : |S_x| \geq C_1 q^{(1-\delta_1)m}\}$. We have

$$|S| = \sum_{x \in T} |S_x| + \sum_{x \notin T} |S_x| \leq |T| q^m + C_1 q^{k+(1-\delta_1)m}.$$

Since $\delta_1 m + 1 \geq \delta_t n$, we have $(1 - \delta_t)n + 1 \geq k + (1 - \delta_1)m$. Similarly, we have $(1 - \delta_t)n + 1 \geq 3m + (1 - \delta_{t-1})k$. It follows that

$$|S| \geq C_t q^{(1-\delta_t)n} \geq C_1 q^{k+(1-\delta_1)m} + C_{t-1} q^{3m+(1-\delta_{t-1})k}.$$

Hence, it follows that

$$|T| \geq \frac{|S| - C_1 q^{k+(1-\delta_1)m}}{q^m} \geq q^{2m} C_{t-1} q^{(1-\delta_{t-1})k}.$$

For every $x \in T$, there is a line ℓ contained in S_x . Since the number of lines in $\mathbb{F}_q^m$ is less than q^{2m} , there is a subset $T' \subseteq T$ of size $|T'| \geq |T| q^{-2m}$ and a line $\ell \subseteq \mathbb{F}_q^m$ such that $\ell \subseteq S_x$ for all $x \in T'$. Since $|T'| \geq C_{t-1} q^{(1-\delta_{t-1})k}$ there is a $(t-1)$ -dimensional subspace $V \subseteq T'$. Hence $\{(x, y) : x \in V, y \in \ell\}$ is a t -dimensional subspace contained in S . $\square$

We restate Theorem B.

Theorem 28. *Let $q \in \{2, 3\}$ and let $A \in \mathbb{F}_q^{m \times k}$ be a row-balanced matrix of rank m . Then $Ax^\top = 0$ is temperate.*

Proof. Let $d = k - m - 1$. Then $\mathbb{F}_q^d$ contains a generic solution y to $Ax^\top = 0$ by Lemma 10. So y has affine rank $m - k$.

Now let $n \geq n_d$ and let $S \subseteq \mathbb{F}_q^n$ have size $|S| \geq C_d q^{(1-\delta_d)n}$. Then S contains a d -dimensional affine subspace $V = \{b_0 + \alpha_1 b_1 + \dots + \alpha_d b_d : \alpha_1, \dots, \alpha_d \in \mathbb{F}_q\}$. Setting $x_i = b_0 + y_{i1} b_1 + \dots + y_{id} b_d$, we obtain a solution to $Ax^\top = 0$ where x has affine rank $k - m$ and $x_1, \dots, x_k \in S$. $\square$

7 Affine copies

Given a balanced matrix $A \in \mathbb{F}_q^{m \times k}$ of rank m , there is a generic solution $z = (z_1, \dots, z_k)$ to $Ax^\top = 0$ in $\mathbb{F}_q^{k-m-1}$ by Lemma 10. Conversely, if $z = (z_1, \dots, z_k) \in (\mathbb{F}_q^r)^k$, then z is a generic solution to $Ax^\top = 0$, where $A \in \mathbb{F}_q^{m \times k}$ has rows that are a basis of $\text{Ann}_{\text{bal}}(z)$. Instead of saying that $S \subseteq \mathbb{F}_q^n$ has a generic solution to $Ax^\top = 0$, we can equivalently say that S contains an affine copy of z . Thus, we can reformulate Theorem A and Theorem B and obtain Corollary C.

Definition 29. Let $z_1, \dots, z_k \in \mathbb{F}_q^r$ and $x_1, \dots, x_k \in \mathbb{F}_q^n$. We say that $x = (x_1, \dots, x_k)$ is an *affine copy* of $z = (z_1, \dots, z_k)$ if there is an injective linear map $L : \mathbb{F}_q^r \rightarrow \mathbb{F}_q^n$ and a vector $a \in \mathbb{F}_q^n$ such that $x_i = L(z_i) + a$ for all $i \in [k]$.

Note that if x is an affine copy of z , then any translate of x is an affine copy of any translate of z .

Lemma 30. Let $z = (z_1, \dots, z_k) \in (\mathbb{F}_q^r)^k$. Let $A \in \mathbb{F}_q^{m \times k}$ be such that the rows form a basis of $\text{Ann}_{\text{bal}}(z)$. Let $n \geq r$ and let $x = (x_1, \dots, x_k) \in (\mathbb{F}_q^n)^k$. Then x is an affine copy of z if and only if x is a generic solution to $Ax^\top = 0$.

Proof. By translating, we may assume without loss of generality that $z_k = 0$ and $x_k = 0$. Note that $z = (z_1, \dots, z_k)$ is a generic solution to $Ax^\top = 0$.

Suppose that x is an affine copy of z . Then $x_i = L(z_i)$ for all $i \in [k]$, where $L : \mathbb{F}_q^r \rightarrow \mathbb{F}_q^n$ is an injective linear map. It is easy to verify that $\text{Ann}_{\text{bal}}(x) = \text{Ann}_{\text{bal}}(z)$. So x is a generic solution to $Ax^\top = 0$.

Conversely, suppose that x is a generic solution to $Ax^\top = 0$. Define $L : \text{span}\{z_1, \dots, z_{k-1}\} \rightarrow \text{span}\{x_1, \dots, x_{k-1}\}$ by

$$L\left(\sum_{i \in [k-1]} \lambda_i z_i\right) := \sum_{i \in [k-1]} \lambda_i x_i.$$

This is a well-defined injective linear map, since

$$\begin{aligned} \sum_{i \in [k-1]} \lambda_i z_i = 0 &\iff (\lambda_1, \dots, \lambda_{k-1}, -\sum_{i \in [k-1]} \lambda_i) \in \text{Ann}_{\text{bal}}(z) \\ &\iff (\lambda_1, \dots, \lambda_{k-1}, -\sum_{i \in [k-1]} \lambda_i) \in \text{Ann}_{\text{bal}}(x) \\ &\iff \sum_{i \in [k-1]} \lambda_i x_i = 0. \end{aligned}$$

Since $n \geq r$, we can extend L to an injective linear map $\mathbb{F}_q^r \rightarrow \mathbb{F}_q^n$. So x is an affine copy of z . □

We can now prove Corollary D as a direct consequence of Theorem A and Theorem B.

Proof of Corollary D. Let $A \in \mathbb{F}_q^{m \times k}$ be a matrix such that the rows form a basis of $\text{Ann}_{\text{bal}}(z_1, \dots, z_k)$. So $z = (z_1, \dots, z_k)$ is a generic solution to $Ax^\top = 0$. If $q \notin \{2, 3\}$, then the premise of Corollary D implies by Lemma 11 that for every $i \in [k]$ the matrix A has two disjoint bases in $[k] \setminus \{i\}$. Hence, by Lemma 13, the matrix A is tame.

By Lemma 30, it follows directly from Theorem A and Theorem B that there is a $\delta > 0$ such that any subset $S \subseteq \mathbb{F}_q^n$ without affine copy of z has size $|S| = O(q^{(1-\delta)n})$. □

8 Concluding remarks

An advantage of considering generic solutions over $(\star)$ -shapes, is that they can be used to obtain not just one, but many solutions given a sufficiently large set $S \subseteq \mathbb{F}_q^n$. In particular, we obtain Corollary C which we restate here.

Corollary 31. *Suppose that the coefficient matrix A of $(\star)$ is tame. Then there exist $\delta > 0$ and $C > 0$ such that for all positive $\delta' < \delta$ the following holds: if $S \subseteq \mathbb{F}_q^n$ has size $|S| \geq q^{(1-\delta')n}$, then S has $\Omega(q^{(k-m)n-C\delta'n})$ solutions to $(\star)$.*

Proof. This follows directly from Theorem 5 and Proposition 22. □

We conclude with an open problem for which we think both a positive and a negative answer would be very interesting.

Open problem 32. *Is it true that $(\star)$ is temperate for all balanced matrices A ?*

A positive answer would be a very strong result, since we do not even know if the system corresponding to 4-term progressions is temperate. As a final note, we remark that the situation where A is tame, corresponds to a strict subset of systems of linear forms of Cauchy-Schwarz complexity 1 (see: [13]). Perhaps this class would be a good candidate for proving a generalisation.

References

- [1] Jonah Blasiak, Thomas Church, Henry Cohn, Joshua A. Grochow, Eric Naslund, William F. Sawin, and Chris Umans. On cap sets and the group-theoretic approach to matrix multiplication. *Discrete Analysis*, 2017(3):1–27, 2017. 3
- [2] Joseph E. Bonin and Hongxun Qin. Size functions of subgeometry-closed classes of representable combinatorial geometries. *Discrete Mathematics*, 224(1-3):37–60, 2000. 4, 19
- [3] Jop Briët. Personal communication. 19
- [4] Ernie Croot, Vsevolod F. Lev, and Péter Pál Pach. Progression-free sets in $\mathbb{Z}_4^n$ are exponentially small. *Annals of Mathematics*, 185(1):331–337, 2017. 3, 6
- [5] Josse van Dobben de Bruyn and Dion Gijswijt. On the size of subsets of $\mathbb{F}_q^n$ avoiding solutions to linear systems with repeated columns. *The Electronic Journal of Combinatorics*, 30(4):P4.1, 2023. 2, 4, 5
- [6] Jordan S. Ellenberg and Dion Gijswijt. On large subsets of $\mathbb{F}_q^n$ with no three-term arithmetic progression. *Annals of Mathematics*, 185(1):339–343, 2017. 3
- [7] Hillel Furstenberg and Yitzhak Katznelson. A density version of the Hales-Jewett theorem. *Journal d’Analyse Mathématique*, 57(1):64–119, 1991. 2

- [8] Jacob Fox and László Miklós Lovász. A tight bound for green’s arithmetic triangle removal lemma in vector spaces. In *Proceedings of the Twenty-Eighth Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 1612–1617. SIAM, 2017. 16, 19
- [9] Jacob Fox and Huy Tuan Pham. Popular progression differences in vector spaces II. *Discrete analysis*, 2019(16), 2019. 19
- [10] Robert Fraser. Three-term arithmetic progressions in subsets of f_q^∞ of large fourier dimension. *Annales Fennici Mathematici*, 46(2):1007–1030, 2021. 14
- [11] Jacob Fox and Lisa Sauermann. Erdős-Ginzburg-Ziv constants by avoiding three-term arithmetic progressions. *The Electronic Journal of Combinatorics*, 25(2):P2.14, 2018. 4
- [12] Jim Geelen and Peter Nelson. An analogue of the Erdős-Stone theorem for finite geometries. *Combinatorica*, 35(2):209–214, 2015. 4
- [13] William T Gowers and Julia Wolf. The true complexity of a system of linear equations. *Proceedings of the London Mathematical Society*, 100(1):155–176, 2010. 22
- [14] Vjekoslav Kovač. Popular differences for right isosceles triangles. *The Electronic Journal of Combinatorics*, 28(4):P4.27, 2021. 3
- [15] Masato Mimura and Norihide Tokushige. Avoiding a star of three-term arithmetic progressions. 2019, [arXiv:1909.10507](https://arxiv.org/abs/1909.10507). 4, 5
- [16] Masato Mimura and Norihide Tokushige. Avoiding a shape, and the slice rank method for a system of equations. 2019, [arXiv:1909.10509](https://arxiv.org/abs/1909.10509). 2, 4, 5
- [17] Masato Mimura and Norihide Tokushige. Solving linear equations in a vector space over a finite field II, 2020. Preprint. URL: <http://www.cc.u-ryukyu.ac.jp/~hide/sol2.pdf>. 4, 5
- [18] Masato Mimura and Norihide Tokushige. Solving linear equations in a vector space over a finite field, *Discrete Mathematics*, 344(12):P112603, 2021. 4
- [19] Eric Naslund. Exponential bounds for the Erdős-Ginzburg-Ziv constant. *Journal of Combinatorial Theory, Series A*, 174:P105185, 2020. 4
- [20] Cosmin Pohoata and Oliver Roche-Newton. Four-term progression free sets with three-term progressions in all large subsets. *Random Structures & Algorithms*, 60(4):749–770, 2021. 16
- [21] Imre Z. Ruzsa. Solving a linear equation in a set of integers I. *Acta arithmetica*, 65(3):259–282, 1993. 4
- [22] Lisa Sauermann. Finding solutions with distinct variables to systems of linear equations over $\mathbb{F}_p^n$, *Mathematische Annalen*, 386:1–33, 2023. 3, 4, 5
- [23] Lisa Sauermann. On the size of subsets of $\mathbb{F}_p^n$ without p distinct elements summing to zero. *Israel Journal of Mathematics*, 243(1):63–79, 2021. 4

- [24] Alexander Schrijver. *Combinatorial optimization: polyhedra and efficiency*, volume 24. Springer Science & Business Media, 2003. 7
- [25] Endre Szemerédi. On sets of integers containing no k elements in arithmetic progression. *Acta Arith*, 27:199–245, 1975. 2
- [26] Terence Tao. Notes on the “slice rank” of tensors, 2016.
URL: <https://terrytao.wordpress.com/2016/08/24/notes-on-the-slice-rank-of-tensors>. 3
- [27] Terence Tao. A symmetric formulation of the Croot-Lev-Pach-Ellenberg-Gijswijt capset bound, 2016. URL: <https://terrytao.wordpress.com/2016/05/18/a-symmetric-formulation-of-the-croot-lev-pach-ellenberg-gijswijt-capset-bound>. 3
- [28] Terence Tao and Van H Vu. *Additive combinatorics*, volume 105. Cambridge University Press, 2006. 14

AUTHOR

Dion Gijswijt
Delft Institute of Applied Mathematics
Delft, The Netherlands
d.c.gijswijt@tudelft.nl
<https://diamhomes.ewi.tudelft.nl/~dgijswijt/>