The Rado Multiplicity Problem in Vector Spaces over Finite Fields

Juanjo Rué[*] Christoph Spiegel[†]

June 24, 2023

1 Introduction

In 1959 Goodman [7] proved that asymptotically at least a quarter of all vertex triples in any graph must either form a clique or an independent set. This lead to the study of the *Ramsey multiplicity problem*, where one would like to determine the minimum number of monochromatic cliques of prescribed size over any edge-coloring of the complete graph [5, 15, 2]. Recently there has been an increased interest in studying the arithmetic analogue of this type of question, originally initiated when Graham, Rödl, and Ruczinsky [8] gave an asymptotic lower bound for the minimum number of monochromatic Schur triples in 2-colorings of the first n integers in 1996, see also [12, 14, 4, 1].

In this extended abstract, we focus on the analogue of the Ramsey multiplicity problem for specific additive structures in vector spaces over finite fields of small order. Let $q \in \mathbb{N}$ be a fixed prime power throughout and write $\mathbb{F}_q$ for the finite field with q elements. Given a subset $T \subseteq \mathbb{F}_q^n$ and a linear map L defined by some matrix $A \in \mathcal{M}^{r\times m}(\mathbb{Z})$ with integer entries co-prime to q, we are interested in studying the set $\mathcal{S}_L(T) = \{\mathbf{s} = (s_1, \ldots, s_m) \in T^m : L(\mathbf{s}) = \mathbf{0} \text{ and } s_i \neq s_j \text{ for } i \neq j\}$ of solutions with all-distinct entries in T. Throughout, we will assume that A is of full rank and that $\mathcal{S}_L(\mathbb{F}_q^n) \neq \emptyset$. We will also write $s_L(T) = |\mathcal{S}_L(T)|/|\mathcal{S}_L(\mathbb{F}_q^n)|$. Writing $[c] = \{1, \ldots, c\}$ for some given number of colors $c \in \mathbb{N}$, we call $\gamma : \mathbb{F}_q^n \to [c]$ a *c-coloring* of dimension $\dim(\gamma) = n$ and let $\gamma^{(i)}$ denote the set of elements colored with color $1 \leq i \leq c$ as well as $\Gamma_c(q, n)$ for the set of all c-colorings of $\mathbb{F}_q^n$. The *Rado multiplicity problem* (to coin a

[*]Departament de Matemàtiques and Institut de Matemàtiques (IMTech) de la Universitat Politècnica de Catalunya (UPC), and Centre de Recerca Matemàtica (CRM), Barcelona, Spain. Spain. E-mail: juan.jose.rue@upc.edu This work was partially funded by the grants MTM2017-82166-P, PID2020-113082GBI00, and the Severo Ochoa and María de Maeztu Program for Centers and Units of Excellence in RD (CEX2020-001084-M).

[†]Zuse Institute Berlin, Department AIS2T, Germany. E-mail: spiegel@zib.de. This work was partially funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy – The Berlin Mathematics Research Center MATH+ (EXC-2046/1, project ID: 390685689).

term analogous to that used in graph theory) is concerned with determining

$$m_c(L, q) = \lim_{n\to\infty} \min_{\gamma\in\Gamma_c(q,n)} s_L(\gamma^{(1)}) + \ldots + s_L(\gamma^{(c)}). \tag{1}$$

The limit exists by monotonicity and we have $0 \le m_c(L, q) \le 1$ by definition. Rado's theorem establishes that $m_c(L, q) > 0$ and we say that L is *c-common* for q if $m_c(L, q) = c^{1-m}$, that is if the minimum number of monochromatic solutions is attained in expectation by a uniform random coloring. For $r = 1$ a result of Cameron, Cilleruelo, and Serra [1] establishes that any L is 2-common if m is odd. When m is even, Saad and Wolf [13] showed that any L where the coefficients can be partitioned into pairs, with each pair summing to zero, is 2-common. Fox, Pham, and Zhao [6] showed that this sufficient condition is in fact also necessary. The case when $r > 1$ is much less understood, with Kamčev, Liebenau, and Morrison [9] recently characterizing a large family of non-common linear maps by showing that any L that 'induces' some smaller 2×4 linear map is uncommon. Focusing on specific values of q, Král, Lamaison, and Pach [10] also recently characterized the 2-common L for $q = 2$ when $r = 2$ and m is assumed to be odd. When $q = 5$, the most relevant additive structures to study is that of 4-APs. Saad and Wolf [13] showed that they are not 2-common by establishing an upper bound of $1/8 - 7 \cdot 2^{10} \cdot 5^{-2} \approx 0.1247 < 2^{-4}$. We establish the first non-trivial lower bound for this problem along with a significantly improved upper bound.

Proposition 1. *We have* $1/10 < m(L_{4\text{-}AP}, 5) \le 13/126 = 0.1\overline{031746}$.

Going beyond 4-APs, we can also show that $m(L_{5\text{-AP}}, 5) \le 1/26 < 2^{-4}$, establishing that 5-APs are likewise not 2-common in $\mathbb{F}_5$, but in this case did not obtain any meaningful lower bound. The study of monochromatic structures in colorings with more than two colors has also proven relevant in extremal graph theory. Most notably, Cummings et al. [3] extended the results of Goodman [7] by establishing the exact Ramsey multiplicity of triangles in 3-colorings and showing that they are not 3-common despite being 2-common. We consider a similar question in the additive setting and establish the exact Rado multiplicity of 3-APs in 3-colorings of $\mathbb{F}_3^n$, likewise showing that they are not 3-common.

Theorem 2. *We have* $m_3(L_{3\text{-}AP}, 3) = 1/27$.

We can also show that $0.04486 \le m_3(L_{\text{Schur}}, 2) \le 1/16$ as well as $m_3(L_{\text{Schur}}, 3) \le 7/81$, establishing that Schur triples are also not 3-common for $q = 2$ and $q = 3$. Upper bounds of all results are obtained through explicit blowup-type constructions. Lower bounds in the graph theoretic setting have recently been obtained through a computational approach relying on flag algebras due to Razborov [11]. This approach has been extended to different contexts, but so far seems to not have been explored in the arithmetic setting. We take a first step in that direction by developing the required theory in the finite-field model and applying it to obtain the above mentioned results. In the following we will briefly touch upon the key concepts necessary to obtain the above results, that is an appropriate notion of isomorphism of colorings that allow us to consider partially labelled objects and for which a basic averaging equality holds, a notion of solution to linear maps to which the flag algebra framework can be applied, a formal definition of the flag algebras as well as a brief remark on how blow-ups are defined in the additive context.

2 The correct notion of isomorphism

Let us omit q and c from notation, so in particular we write $\Gamma(n) = \Gamma_c(q,n)$ for the set of all c-colorings of dimension n as well as $\Gamma = \bigcup_{n=0}^{\infty} \Gamma(n)$. The 0-dimensional vector space consist of a single point, that is $\mathbb{F}_q^0 = \{0\}$, and we write e_j for the j-th canonical unit basis vector of $\mathbb{F}_q^n$ for $1 \leq j \leq n$ as well as e_0 for the zero vector.

Definition 3. *We refer to an affine linear map* $\varphi : \mathbb{F}_q^k \to \mathbb{F}_q^n$ *as a* morphism *and say that it is* t-fixed *for some* $t \geq 0$ *if* $\varphi(e_j) = e_j$ *for all* $0 \leq j \leq t$*. A morphism is a* monomorphism *whenever it is injective and a monomorphism is an* isomorphism *whenever* $n = k$*.*

Out of notational convenience, we extend the range of t to -1 in order to include *unfixed* morphisms and will always use t^+ to denote $\max\{t, 0\}$. For a given $t \geq -1$ and $n \geq k \geq t^+$, we let $\mathrm{M}_t(k;n)$ denote the set of t-fixed morphisms from $\mathbb{F}_q^k$ to $\mathbb{F}_q^n$ up to t-fixed isomorphism of $\mathbb{F}_q^k$. We likewise write $\mathrm{Mon}_t(k;n)$ for the set of monomorphisms with the same properties. We will also refer to the image of an element of $\mathrm{Mon}_t(k;n)$ as a *t-fixed k-dimensional subspace* of $\mathbb{F}_q^n$, so that 0-fixed subspaces correspond to linear subspaces and unfixed subspaces correspond to *affine* subspaces. Given $k_1, \ldots, k_m \geq t^+$ and $n \geq k_1 + \ldots + k_m - (m-1)\, t^+$, we let $\mathrm{Mon}_t(k_1, \ldots, k_m; n)$ denote the set of all tuples of monomorphisms $(\varphi_1, \ldots, \varphi_m) \in \mathrm{Mon}_t(k_1;n) \times \ldots \times \mathrm{Mon}_t(k_m;n)$ only overlapping in the t-fixed subspace.

Using these notions, we say two colorings $\gamma_1, \gamma_2 \in \Gamma(n)$ are *t-fixed isomorphic* for some $t \geq -1$, denoted by $\gamma_1 \cong_t \gamma_2$, if there exists a t-fixed isomorphism $\varphi : \mathbb{F}_q^n \to \mathbb{F}_q^n$ satisfying $\gamma_1 \equiv \gamma_2 \circ \varphi$. We let $\Gamma_t(n) = \Gamma(n)/\cong_t$ denote the set of all c-colorings of $\mathbb{F}_q^n$ up to t-fixed isomorphism and also write $\Gamma_t = \bigcup_{n \geq t^+} \Gamma_t(n)$. Given $k_1, \ldots, k_m \geq t^+$ and $n \geq k_1 + \ldots + k_m - (m-1)\, t^+$, the *density* $p_t(\delta_1, \ldots, \delta_m; \gamma)$ of some colorings $\delta_1 \in \Gamma_t(k_1)$, ..., $\delta_m \in \Gamma_t(k_m)$ in $\gamma \in \Gamma_t(n)$ is defined as the probability that a a tuple of t-fixed monomorphism chosen uniformly at random from $\mathrm{Mon}_t(k_1, \ldots, k_m; n)$ induces copies of $\delta_1, \ldots, \delta_m$ in γ. For $n \geq k \geq t^+$, we also let the *degenerate density* $p_t^d(\delta; \gamma)$ of some $\delta \in \Gamma_t(k)$ in γ denote the probability that a not-necessarily-injective t-fixed morphism does the same. Note that asymptotically

$$p_t^d(\delta; \gamma) = p_t(\delta; \gamma)\,(1 + o_n(1)) \tag{2}$$

when $n \to \infty$ and that for $n \geq n' \geq k_1 + \ldots + k_m - (m-1)\, t^+$ we also have

$$p_t(\delta_1, \ldots, \delta_m; \gamma) = \sum_{\beta \in \Gamma_t(n')} p_t(\delta_1, \ldots, \delta_m; \beta)\, p_t(\beta; \gamma). \tag{3}$$

3 The correct notion of solution

In order to develop the flag algebra approach, the density of solutions needs to be representable as the weighted density of particular colorings, motivating the following definition.

Definition 4. *For any $t \geq -1$ and $n \geq t^+$, the* t-fixed dimension $\dim_t(s)$ *of* $\mathbf{s} \in \mathcal{S}_L(\mathbb{F}_q^n)$ *is the smallest $k \geq t^+$ for which there exists a t-fixed k-dimensional subspace of $\mathbb{F}_q^n$ containing* $\mathbf{s}$.

We will only need the unfixed and 0-fixed dimension and denote by $\dim_t(L)$ the largest t-fixed dimension of any solution to a given linear map L. In general, $\dim_t(L) = m-r+t$ for any linear map L when $t \geq 0$ as well as $\dim_{-1}(L) = m-r-1$ when L is *invariant*, that is if for any solution $\mathbf{s} = (x_1, \ldots, x_m) \in \mathcal{S}_L(\mathbb{F}_q^n)$ and element $a \in \mathbb{F}_q^n$ we have $a + \mathbf{s} = (a + x_1, \ldots, a + x_m) \in \mathcal{S}'_L(\mathbb{F}_q^n)$. We say that L is *admissible* if $t \geq 0$ or if $t = -1$ and L is invariant. A solution $\mathbf{s} \in \mathcal{S}_L(\mathbb{F}_q^n)$ for some admissible L is *t-fixed fully dimensional* if $\dim_t(s)$ attains the respective upper bound. For a given set $T \subseteq \mathbb{F}_q^n$, we denote the set of fully dimensional solutions to some admissible L by $\mathcal{S}_L^t(T)$ and write $s_L^t(T) = |\mathcal{S}_L^t(T)| \,/\, |\mathcal{S}_L^t(\mathbb{F}_q^n)|$. Note that $\mathcal{S}_L^t(\mathbb{F}_q^n)| = |\mathcal{S}(\mathbb{F}_q^n)| \,\big(1 + o(1)\big)$.

The important property that we make use of is that each fully-dimensional solution defines a unique $\dim(L)$-dimensional t-fixed subspace in which it lies and that for any $t \geq -1$, admissible L, and $n \geq t \geq 0$, the number of solutions in a subset of $\mathbb{F}_q^n$ is invariant under t-fixed isomorphism. The same would not hold for $t = -1$ if L was not invariant. In general we therefore need to consider 0-fixed morphisms, but whenever exclusively dealing with invariant structures, we can be more economical, as unfixed morphisms lead to a smaller number of isomorphism classes of colorings. Finally, let us note that fully-dimensional solutions satisfy

$$s_L^t(\gamma^{(i)}) = \sum_{\delta \in \Gamma_t(k)} s_L^t(\delta^{(i)})\, p_t(\delta; \gamma) \tag{4}$$

for any $t \geq -1$, admissible L, $\dim(L) \leq k \leq n$, $\gamma \in \Gamma_t(n)$, and $1 \leq i \leq c$.

4 The flag algebras for additive structures

For any $t \geq 0$, we refer to elements of $\Gamma_t(t) = \Gamma(t)$ as *types* of dimension t. We also introduce a unique *empty type*, denoted by $\varnothing$, of dimension $t = -1$. For a given type τ of dimension t, we refer to a coloring $F \in \Gamma_t(n)$ satisfying $F \circ \mathrm{id}_{t,n} \equiv \tau$ as a *flag of type* τ, where $\mathrm{id}_{t,n}$ denotes the unique t-fixed isomorphism from $\mathbb{F}_q^t$ to $\mathbb{F}_q^n$ and the requirement is vacantly true for $t = -1$. We will write $\mathcal{F}_n^\tau$ for the set of all flags of given type τ and dimension n as well as $\mathcal{F}^\tau = \bigcup_n \mathcal{F}_n^\tau$.

Definition 5. *The* flag algebra $\mathcal{A}^\tau$ *of type τ is given by equipping $\mathbb{R}\mathcal{F}^\tau / \mathcal{K}^\tau$, where $\mathcal{K}^\tau = \{F - \sum_{F' \in \mathcal{F}_n^\tau} p_t(F; F')\, F' : F \in \mathcal{F}^\tau, n \geq \dim(F)\}$, with the product given by the the bilinear extension of $F_1 \cdot F_2 = \sum_{H \in \mathcal{F}_n^\tau} p_t(F_1, F_2; H)\, H + \mathcal{K}^\tau$ defined for any two flags $F_1, F_2 \in \mathcal{F}^\tau$ and arbitrary $n \geq \dim(F_1) + \dim(F_2) - \dim(\tau)$.*

Assume that we are given a parameter $\lambda : \Gamma \to \mathbb{R}$ that is invariant under t_λ-fixed isomorphisms for some $t_\lambda \geq -1$ and that satisfies $\lambda(\gamma) = \sum_{\beta \in \Gamma_{t_\lambda}(n)} \lambda(\beta)\, p_{t_\lambda}(\beta, \gamma)$ for some $n_\lambda \in \mathbb{N}$ and all $\gamma \in \Gamma_{t_\lambda}$, where $n_\lambda \leq n \leq \dim(\gamma)$. Note that monochromatic fully-dimensional solutions to a given linear map L define such a parameter with $t_\lambda = 0$ for general L and $t_\lambda = -1$ for invariant ones, where in either case $n_\lambda = \dim_{t_\lambda}(L)$. We are interested in determining

$$\lambda^\star = \lim_{n \to \infty} \min_{\gamma \in \Gamma_{t_\lambda}(n)} \lambda(\gamma). \tag{5}$$

Writing $C_\lambda^\tau = \sum_{\beta \in \mathcal{F}_{n_\lambda}^\tau} \lambda(\beta)\,\beta$ for any type τ of dimension t_λ, our problem of determining $\lambda^\star$ can be restated through the conic optimization problem

$$\lambda^\star = \max\{\lambda' \in \mathbb{R} : C_\lambda^\tau \geq \lambda' \text{ for all types } \tau \text{ of dimension } t_\lambda\}, \tag{6}$$

where we write $\mathrm{Hom}^+(\mathcal{A}^\tau, \mathbb{R})$ for the set of positive homomorphisms, that is algebra homomorphisms $\phi \in \mathrm{Hom}(\mathcal{A}^\tau, \mathbb{R})$ satisfying $\phi(F) \geq 0$ for any $F \in \mathcal{F}^\tau$, and $\mathcal{S}^\tau = \{f \in \mathcal{A}^\tau : \phi(f) \geq 0 \text{ for all } \phi \in \mathrm{Hom}^+(\mathcal{A}^\tau, \mathbb{R})\}$ for the *semantic cone* of type τ. Noting that we can define a linear *downward operator* $[\![\cdot]\!]_{t_\lambda} \colon \mathcal{A}^\tau \to \mathcal{A}^{\tau_\lambda}$ for any type τ of dimension $t \geq t_\lambda$ that satisfies $[\![\mathcal{S}^\tau]\!]_{t_\lambda} \subseteq \mathcal{S}^{\tau_\lambda}$, we can derive a lower bound by defining a set of types $\mathcal{T}$ as well as sets of algebra elements $\mathcal{B}_{\tau'} \subset \mathcal{A}^{\tau'}$ and establishing that

$$C_\lambda^\tau \geq \lambda' + \sum_{\tau' \in \mathcal{T}} \sum_{f \in \mathcal{B}_{\tau'}} [\![f^2]\!]_{t_\lambda}. \tag{7}$$

5 Blow-ups for upper bounds

While different ways of obtaining upper bounds have been explored, by far the most powerful method is an analogue of the simple graph blow-up. Given $0 \leq k \leq n$, we let $\mathrm{id}_{n,k}$ denote the unique k-fixed morphism for which $\ker \mathrm{id}_{n,k} = \{0\} \times \mathbb{F}_q^{n-k}$. For $t \geq -1$, $t^+ \leq k \leq n$ and $\gamma \in \Gamma_t(k)$, we refer to $\gamma[n] = \gamma \circ \mathrm{id}_{n,k} \in \Gamma_t(n)$ as the n-dimensional *blow-up* of γ. The decisive property of the blow-up is its invariance with respect to the degenerate densities of subcolorings, that is for any $t \geq 1$, $t^+ \leq k_1 \leq k_2 \leq n$, $\delta \in \Gamma_t(k_1)$, and $\gamma \in \Gamma_t(k_2)$, we have $p_t^d(\delta, \gamma[n]) = p_t^d(\delta, \gamma)$. We therefore have

$$\lambda^\star \leq \sum_{\beta \in \Gamma_{t_\lambda}(n_\lambda)} \lambda(\beta)\, p_{t_\lambda}^d(\beta, \delta) \tag{8}$$

for any $k \geq t_\lambda$ and $\delta \in \Gamma_{t_\lambda}(k)$, meaning we can derive an upper bound from any explicit coloring. Going beyond this, one can sometimes use *iterated blow-ups* to obtain a slightly improved value.

6 Concluding Remarks

The above lays the foundation for how to derive the results stated in the introduction. In particular, we note that both Proposition 1 and Theorem 2 were derived considering colorings of $\mathbb{F}_q^2$ with $\mathcal{T}$ consisting of all types of dimension 0 and the $\mathcal{B}_\tau$ respectively consisting 4 and 6 flags. The resulting proofs are compact enough (with respect to the number of variables but not the number of constraints) that rounding the results of the SDP solver `csdp`, commonly one of the biggest technical hurdles with these types of proofs, was reasonably straight-forward even when no matching upper bound was known.

Note that this extended abstract represents preliminary work and that in the future we hope to further develop this line of research, for example by formulating a stability result for Theorem 2 and by examining additional additive problems. At the same time we note that this line of research faces a much steeper hurdle compared to similar problems in graph theory: since the number of underlying objects grows exponentially rather than polynomially (respectively in the dimension and the order), one very quickly faces severe computational limitations. Nevertheless, we hope that future work will continue to develop this framework for problems beyond graph theory.

References

[1] P. J. Cameron, J. Cilleruelo, and O. Serra. On monochromatic solutions of equations in groups. *Revista Matemática Iberoamericana*, 23(1):385–395, 2007.

[2] D. Conlon. On the Ramsey multiplicity of complete graphs. *arXiv preprint arXiv:0711.4999*, 2007.

[3] J. Cummings, D. Král', F. Pfender, K. Sperfeld, A. Treglown, and M. Young. Monochromatic triangles in three-coloured graphs. *Journal of Combinatorial Theory, Series B*, 103(4):489–503, 2013.

[4] B. A. Datskovsky. On the number of monochromatic Schur triples. *Advances in Applied Mathematics*, 31(1):193–198, 2003.

[5] P. Erdős. On the number of complete subgraphs contained in certain graphs. *Magyar Tud. Akad. Mat. Kutató Int. Közl*, 7(3):459–464, 1962.

[6] J. Fox, H. T. Pham, and Y. Zhao. Common and Sidorenko linear equations. *The Quarterly Journal of Mathematics*, 72(4):1223–1234, 2021.

[7] A. W. Goodman. On sets of acquaintances and strangers at any party. *The American Mathematical Monthly*, 66(9):778–783, 1959.

[8] R. Graham, V. Rödl, and A. Ruciński. On Schur properties of random subsets of integers. *Journal of Number Theory*, 61(2):388–408, 1996.

[9] N. Kamčev, A. Liebenau, and N. Morrison. Towards a characterisation of Sidorenko systems. *arXiv preprint arXiv:2107.14413*, 2021.

[10] A. Lamaison, P. P. Pach, et al. Common systems of two equations over the binary field. In *Discrete Mathematics Days 2022*, pages 169–173. Editorial de la Universidad de Cantabria, 2022.

[11] A. A. Razborov. Flag algebras. *The Journal of Symbolic Logic*, 72(4):1239–1282, 2007.

[12] A. Robertson and D. Zeilberger. A 2-coloring of $[1, n]$ can have $(1/22)n^2 + o(n)$ monochromatic Schur triples, but not less! *The Electronic Journal of Combinatorics*, 5(1):R19, 1998.

[13] A. Saad and J. Wolf. Ramsey multiplicity of linear patterns in certain finite abelian groups. *The Quarterly Journal of Mathematics*, 68(1):125–140, 2017.

[14] T. Schoen. The number of monochromatic Schur triples. *European Journal of Combinatorics*, 20(8):855–866, 1999.

[15] A. Thomason. A disproof of a conjecture of Erdős in Ramsey theory. *Journal of the London Mathematical Society*, 2(2):246–255, 1989.