When Separation Fails, a Canon Appears

One counting identity behind separation, synchronization, and symmetry-breaking in permutation groups, formalized in Lean 4 (Part I)

Carles Marín*
Independent researcher
karlesmarin@gmail.com

July 2026

Abstract

One arithmetic identity runs through this paper: the average, over a finite group G acting on Ω, of how many points a translate gA shares with a set B is exactly $|A|\,|B|/|\Omega|$. Read one way it proves P. M. Neumann's separation lemma; read another it forces the uniformity theorems of P. J. Cameron's synchronization hierarchy; and at the boundary $|A|\,|B| = |\Omega|$ it yields a dichotomy—either some g pulls A off B, or *every* translate meets B in exactly one point. That extremal case is an exact factorization of the group, and over $\mathbb{Z}/n$ a rhythmic tiling canon: the boundary of separation theory and the theory of musical canons are the same object, in two literatures that do not cite one another. I formalize this cluster in Lean 4 / Mathlib, together with the *distinguishing number* of a group action and the Fano-plane value $D(\mathrm{GL}_3(\mathbb{F}_2)) = 4$. The mathematics is classical; new here are the orbit-local form of the dichotomy, the identification of its extremal case with rhythmic canons, and—to my knowledge—the first formalization of any of these in a proof assistant. Everything is `sorry`-free, depending only on the three standard axioms: a pearl, and the first part of a planned series.

1 One argument, several faces

Let a finite group G act on a set Ω, and take two finite subsets $A, B \subseteq \Omega$. Applying $g \in G$ slides A to its translate gA. Almost everything in this paper follows from counting, in two ways, the triples (a, b, g) with $a \in A$, $b \in B$, and $g \cdot a = b$. When G acts transitively on Ω, summing over the group and clearing denominators gives the identity

$$\boxed{\Big(\sum_{g \in G} |gA \cap B|\Big) \cdot |\Omega| \;=\; |A| \cdot |B| \cdot |G|}$$

—the average size of $gA \cap B$ is $|A|\,|B|/|\Omega|$; a form local to the orbits holds for any action, and is what the dichotomy of Section 4 needs. It looks like a bookkeeping remark. It is in fact the engine of a surprisingly wide cluster of theorems, and the single message of this paper is that they are one argument seen from different sides (Figure 1).

*Formalized with AI assistance (Claude, Anthropic); the mathematics and all claims are the author's responsibility.

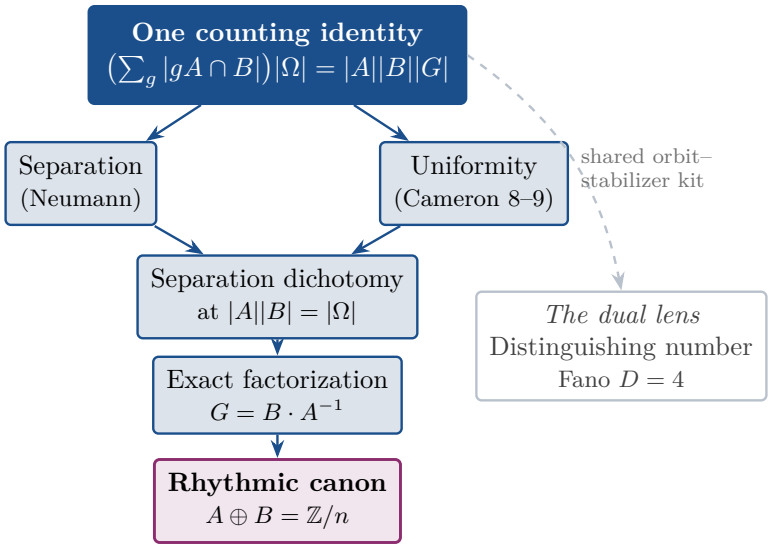


Figure 1: The paper in one picture. A single counting identity forces both Neumann separation and Cameron's uniformity theorems; where they meet, at the threshold $|A||B| = |\Omega|$, it produces a dichotomy whose non-separable case is an exact factorization of the group—over $\mathbb{Z}/n$, a rhythmic tiling canon. The distinguishing number (the Fano exception $D = 4$) is a parallel question about breaking symmetry, sharing the same orbit–stabilizer toolkit.

What is new, in three registers. Because this paper sits between a survey and a formalization, I separate its claims cleanly. *Mathematically*, the new content is a sharpened, orbit-local form of the separation dichotomy (Section 4), and the observation that its extremal case, over a cyclic group, is exactly the rhythmic tiling canon of Vuza [12] and Coven–Meyerowitz [11]. *In a proof assistant*: to the best of my knowledge, after an extensive literature search across the major systems, this is the first formalization of the separation lemma, of Cameron's synchronization hierarchy, and of the distinguishing number of a group action. *Conceptually*, the contribution is to make the shared engine explicit: separation, uniformity, the extremal dichotomy, and the factorization all reduce, by name and in the dependency graph, to the one identity above. Appendix A lists the formal results with their Lean names; the mathematics is classical throughout, and I name its authors as I go.

2 Separating a set from its image

The oldest face of the identity is a question with an intuitive answer:

> *when can we always find a g that pulls A entirely off B—with $gA \cap B = \emptyset$?*

If the orbits are large there is room to slide A clear of B. Neumann made this precise. In the finite transitive case the clean threshold is $|A| \cdot |B| < |\Omega|$: below it, separation is always possible (Figure 2); the counting identity is the whole proof, since if no g separated then every term $|gA \cap B| \geq 1$, forcing the sum to at least $|G|$ and the average to at least 1, i.e. $|A|\,|B| \geq |\Omega|$.

One subtlety earns a sentence, because a popular paraphrase gets it wrong. The threshold is *strict*. The quantitative source—Birch, Burns, Oates Macdonald and Neumann [1]—separates under the hypothesis that every orbit has *more than* $|A|\,|B|$ elements, and notes that $|A|\,|B| + 1$ is best possible: a transitive group of degree $|A|\,|B|$ built from $|A|$ blocks of size $|B|$ has a non-separable pair. Weakening "more than" to "at least" makes the statement false (the trivial group on one point

Table 1: Computational cross-checks (GAP / Sage, exact). *Left:* the separation dichotomy, verified with no counterexample across every transitive group of small degree, plus the $\mathbb{Z}/12$ canon witness. *Right:* an independent recomputation of Chan's distinguishing table $D(\mathrm{GL}_n(\mathbb{F}_q) \curvearrowright \mathbb{F}_q^n)$ for $n > 2$, $q \le n{+}1$, matching Klavžar–Wong–Zhu; cell colour encodes D (pale $D{=}2 \to$ deep $D{=}4$), so the two exceptions stand out at a glance.

Check	Result
dichotomy sweep	0 counterexamples
120 transitive grps, deg. 2–9	
$\mathbb{Z}/12$ canon $\{0,3,6,9\}\oplus\{0,1,2\}$	tiles (extremal)

$n\backslash q$	2	3	4	5
3	**4**	2	2	—
4	**3**	2	2	2
5	2	2	2	2
6	2	2	2	2

$D{=}2$ $D{=}3$ $D{=}4$ ("—": q not a prime power)

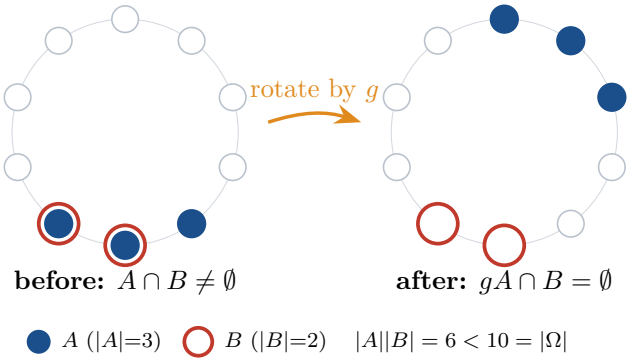


Figure 2: Separation on a decagon (regular $\mathbb{Z}/10$ action). Since $|A| \cdot |B| < |\Omega|$, some rotation slides A (blue) off B (red rings). The threshold $|A||B| = |\Omega|$, where separation can fail, is where the story turns (Section 4).

never separates), and the boundary case $|A|\,|B| = |\Omega|$—where the strict lemma is silent—is exactly where Section 4 lives.

For infinite Ω the right hypothesis is on orbits, and the sharp form asks only that the orbit of every point of A be infinite. The proof is the pleasant dual of the finite one: if no g separated, the cosets $\{g \mid g \cdot a = b\}$ would cover G, so by B. H. Neumann's covering lemma [2] some point stabilizer would have finite index—but its index is the (infinite) orbit size. Mathlib already carries B. H. Neumann's covering lemma; the group-action wrapper it was missing is supplied here.

3 Uniformity: the same average, read as an equality

Cameron's synchronization lectures [4] turn the identity into a family of rigidity statements. If every translate-intersection happens to have the *same* size ℓ, the identity immediately gives $|A|\,|B| = \ell\,|\Omega|$; its $\ell = 1$ instance says a section-regular partition is uniform, every part the same size. Sharper, and the fact that drives the next section: if all the intersections are merely $\ge \ell$ (or all $\le \ell$) while $|A|\,|B| = \ell\,|\Omega|$, then every one of them equals ℓ exactly.

The remarkable point is worth stating in plain words. An average is a statement about a *sum*; here it reaches down and pins every individual term. Because the mean of the $|gA \cap B|$ is forced to be exactly ℓ, no single translate can sit above or below it without another compensating—so once a one-sided bound removes that freedom, the average dictates each term on its own. It is an average

that legislates pointwise.

I am careful about what this "unification" is. I did not prove one meta-theorem with separation, uniformity, and the dichotomy as corollaries; rather, all three call the same triple-count. The unity is real but modest, and it lives in the dependency graph, not in a grand statement—which is precisely the kind of claim a formalization lets a reader check rather than take on faith.

4 When separation fails: a dichotomy, and a canon

Return to the boundary $|A| \cdot |B| = |\Omega|$, where the strict separation lemma says nothing. Here the engine forces a clean fork.

Theorem 1 (Separation dichotomy, orbit-local form)**.** *Let G be finite acting on Ω, and A, B nonempty finite with every orbit meeting both A and B of size $\geq |A| \cdot |B|$. Then either*

(1) *some g separates A from B, or*

(2) (extremal) $|gA \cap B| = 1$ *for* every $g \in G$*, and A and B lie in a single common orbit of size exactly $|A| \cdot |B|$.*

The proof is the average once more: if no g separates, every term is ≥ 1; the identity fixes their mean at 1; so by the pointwise squeeze of the previous section every $|gA \cap B|$ is exactly 1, and the equality case collapses $A \cup B$ into one orbit of the extremal size. Strictly above threshold one gets separation outright.

I state the honesty plainly, because the fork's transitive core is not mine. That $|A|\,|B| = |\Omega|$ forces either separation or all-intersections-one is, essentially verbatim, the definition of a *separating group* in Araújo–Cameron–Steinberg [3]. What I claim is the orbit-local, weak, non-transitive form above—the hypothesis constrains only the orbits meeting both sets, and the conclusion *produces* the single common orbit—and its formalization.

The extremal case is a factorization. What are the extremal pairs? For the regular action of G on itself, "$|gA \cap B| = 1$ for all g" says exactly that every group element is uniquely $b\,a^{-1}$ with $a \in A$, $b \in B$: an *exact factorization* $G = B \cdot A^{-1}$. Written additively for $G = \mathbb{Z}/n$ it makes the difference map $(a, b) \mapsto b - a$ a bijection; equivalently, since $|A|\,|B| = n$, the translates $\{A + b : b \in B\}$ partition $\mathbb{Z}/n$—the tiling $A \oplus B = \mathbb{Z}/n$. Such a tiling is a *rhythmic canon*: a rhythm A and a set of entry times B whose shifted copies cover every beat once, with no gap and no clash (Figure 3). A non-separable extremal pair *is* a canon.

I flag the near neighbors so a referee need not. The idea "non-separation = factorization" appears, for diagonal actions, in Araújo–Cameron–Steinberg [3] (perfect factorizations of simple groups), and for the $A = B$ case in Barbieri et al. [5] (difference sets and projective planes). What seems unremarked is the identification of the two-set regular extremal case over $\mathbb{Z}/n$ with rhythmic tiling canons: the separation literature and the tiling literature (Vuza [12], Coven–Meyerowitz [11], Amiot [14]) do not cite one another. The connection is novel as an *observation*, not as mathematics; its value is that it is now a lemma rather than an analogy—which is what a proof assistant is for.

5 The dual question: how much symmetry must you break?

So far the counting engine has measured how a group *moves* sets—how far it can push A off B. A mirror quantity measures how hard the action is to *pin down*: how much labeling it takes to remove

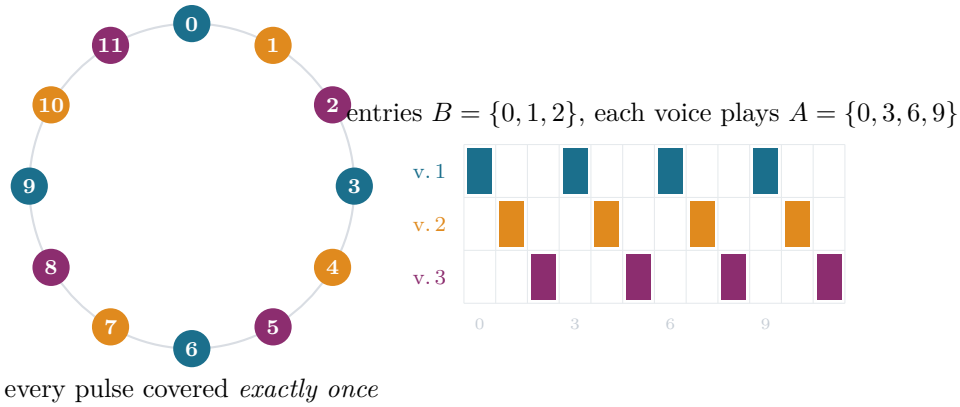


Figure 3: The extremal (non-separable) pair $A = \{0, 3, 6, 9\}$, $B = \{0, 1, 2\}$ on $\mathbb{Z}/12$ is a rhythmic canon. Left: the three translates A (teal), $A{+}1$ (amber), $A{+}2$ (violet) partition the twelve pulses—no gap, no overlap. Right: as music, three voices enter one beat apart, each playing the rhythm A. A sonified version accompanies the companion music-theory note.

its symmetry entirely. I view the two as opposite ends of one programme—separation adds room until the group can move a set clear; distinguishing adds colours until the group can move nothing at all—and a single inequality proved below joins them: a base of size b (a set whose pointwise stabilizer is trivial) gives $D \le b + 1$, the bound that ties distinguishing to the base and matroid theory (IBIS) forming the spine of Part II. That is why the topic belongs here, as the counting programme's dual face rather than an appendix.

Color the points of Ω; the coloring is *distinguishing* if the identity is the only element of G that preserves it, and the *distinguishing number* $D(G \curvearrowright \Omega)$ is the fewest colors that suffice (Albertson–Collins [7]; Tymoczko [8] for general actions). Mathlib had no notion of it; the definition, its monotonicity, and the base bound $D \le b + 1$ are supplied here.

For $\mathrm{GL}_n(\mathbb{F}_q)$ acting on the nonzero vectors of $\mathbb{F}_q^n$, how many colors does it take?

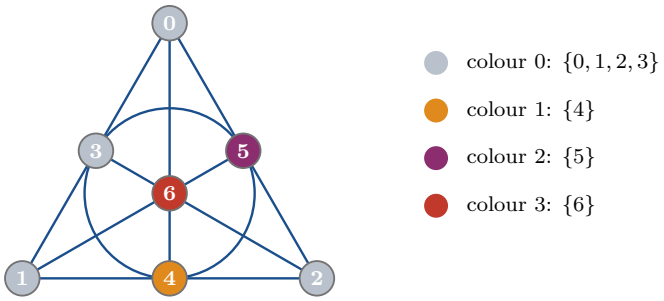
Melody Chan asked exactly this [9]; the answer is Klavžar–Wong–Zhu [10]: two colors always suffice, with four exceptions, of which the unique maximum is $D(\mathrm{GL}_3(\mathbb{F}_2)) = 4$. That group, of order 168, is the collineation group of the Fano plane on its seven points, and the exceptional value is the one I verify (Figure 4).

The surprise is the size of the gap. For every larger linear action two colors break all the symmetry; here, on just seven points, even *three* colors cannot—every one of the $3^7 = 2187$ three-colorings is preserved by some collineation—while a specific four-coloring does. The lower bound is the exhaustive half: twenty-one collineations suffice to fix every three-coloring between them, checked by the kernel. The upper bound is pure geometry: three points wear unique colors and are pinned, three lines through them pin three more, and injectivity pins the last. The Fano plane is small enough to see and just large enough to be rigid.

6 Why this matters

I address three readers directly, because the work speaks to each differently.

To a permutation-group theorist. The extremal case of separation is usually met as a curiosity at the boundary of a threshold theorem. Reading it as an exact factorization, and then as a tiling,



no 3-colouring kills all 168 collineations; this 4-colouring does

Figure 4: The Fano plane (7 points, 7 lines), whose 168 collineations are $\mathrm{GL}_3(\mathbb{F}_2)$ on the nonzero vectors of $\mathbb{F}_2^3$. The unique colours $1, 2, 3$ pin points $4, 5, 6$; three lines then pin $2, 0, 1$ and injectivity pins 3. Hence $D = 4$.

connects it to a large and active body of work—Vuza's aperiodic canons [12], the Coven–Meyerowitz conditions [11], Fuglede's spectral-set question [13]—that the synchronization literature does not currently draw on. The dictionary runs both ways: constructions of aperiodic tilings become constructions of non-separable extremal pairs, and vice versa. The orbit-local form of the dichotomy is also, I believe, the natural statement—it needs neither transitivity nor a global orbit bound.

To someone building mathematics in Lean. These foundations were not previously available in a proof assistant. The averaging identity, the uniformity theorems, the base bound $D \le b+1$, and the distinguishing-number API are now reusable; they are exactly the pieces on which the matroid (IBIS) theory of Part II is built. Mathlib gains a small but load-bearing corner of permutation-group combinatorics it did not have.

To someone in synchronization theory. The separating/synchronizing hierarchy is defined through precisely the intersection condition studied here. Making the counting engine and the extremal dichotomy formal, and tying the extremal case to a well-developed tiling theory, offers the field both a checked foundation and a source of examples and non-examples it has not been mining. The $\mathbb{Z}/n$ canons are an inexhaustible supply of extremal pairs.

7 Where I stopped

This is the first cluster of a series, honestly mapped, not a finished theory. Done: Neumann separation (finite and infinite); the counting engine and the uniformity theorems; the orbit-local dichotomy with the factorization and rhythmic-canon identification; distinguishing numbers, their API, and the Fano exception. Ahead, and pinned but not yet built: the IBIS theorem of Cameron–Fon-Der-Flaass [6] (irredundant bases of constant size are a matroid), the central brick of Part II and the natural home of the base bound proved here; the explicit bridge lemmas that turn this cluster from a list into a fabric; and Chan's remaining distinguishing values, together with the apparently untreated projective analogue $D(\mathrm{PGL}_n(\mathbb{F}_q) \curvearrowright \mathrm{PG}^{n-1})$. The road is classical, but unbuilt.

8 Related work

The mathematics is classical: the separation lemma is Birch–Burns–Oates Macdonald–Neumann [1] and Neumann's infinite version; the counting hierarchy and the separating/synchronizing dichotomy are Cameron's and Araújo–Cameron–Steinberg's [3]; the $A = B$ extremal theory is Barbieri et al. [5]; distinguishing numbers are Albertson–Collins and, for linear groups, Chan [9] and Klavžar–Wong–Zhu [10]; the tiling side is Vuza and Coven–Meyerowitz. On the formal side, Mathlib provides group actions, orbit–stabilizer, Burnside, matroids, and B. H. Neumann's coset-covering lemma, but none of the separation lemma, the synchronization hierarchy, or distinguishing numbers; I am aware of no prior machine-checked treatment of these in any prover.

9 Conclusion

One counting identity, viewed through different lenses, generates separation, synchronization, exact factorizations, rhythmic canons, and—through the dual question of coloring—symmetry-breaking. Formalization does not create this unity; it makes it explicit, and checkable, and it turns the crossing between permutation groups and musical canons from an analogy into a theorem. None of the mathematics is new; the contribution is that it now lives in a proof assistant, and that the shared engine is visible in the dependency graph rather than asserted. Each new piece arose from looking at the case a classical theorem leaves aside—the equality in a strict inequality, the boundary of a threshold—which is often where an unnamed object sits. I offer this as a pearl, and as the first part of a series.

Part II takes up the one brick this paper only names: the theorem of Cameron and Fon-Der-Flaass that a permutation group whose irredundant bases all have the same size carries a matroid on its points. It is the structural heart the base bound $D \leq b + 1$ already points to, and with it the pieces gathered here—separation, counting, uniformity, distinguishing—become a single connected chapter rather than a first stone. The counting identity of Section 1 will still be underneath; the aim of the series is to keep making such shared engines visible, one checked brick at a time.

On method. This development was carried out with AI assistance (Claude, Anthropic): definitions, lemmas, and tactics were proposed and then accepted or rejected against the kernel. The scope-keeping of this paper—the classical cores named as such, the one value I could not feasibly prove in Lean (the order 168) flagged and cross-checked in GAP rather than asserted—reflects that the kernel, not the assistant, has the last word.

Artifacts. All Lean sources (`sorry`-free; the axiom report is in Table 2), the GAP cross-checks of Table 1, and the figures are available at `https://github.com/karlesmarin/godsil-gutman-lean`, archived at DOI 10.5281/zenodo.21419285.

A The formal results

Table 2 lists every formalized statement with its Lean name and status. All theorems are `sorry`-free and non-vacuous, and `#print axioms` reports only `propext`, `Classical.choice`, `Quot.sound` (the exhaustive cover `fanoWitnesses_cover` needs even less). The three ◦ future rows are the frontier mapped in Section 7.

Table 2: The formalised results (Lean 4 / Mathlib).

Lean name	Statement	Status
`separation_lemma_of_pretransitive`	$\lvert A\rvert\lvert B\rvert < \lvert\Omega\rvert \Rightarrow \exists g,\ gA \cap B = \emptyset$	✓ proven
`neumann_separation_lemma`	orbits of A infinite $\Rightarrow$ separable	✓ proven
`sum_card_smul_inter_mul_card`	$(\sum_g \lvert gA \cap B\rvert)\,\lvert\Omega\rvert = \lvert A\rvert\lvert B\rvert\lvert G\rvert$ (Cameron Thm 10)	✓ proven
`card_smul_inter_eq_of_forall_le`	average-equals-extremum squeeze (Cameron Thm 8)	✓ proven
`IsSectionRegular.card_part_mul...`	section-regular $\Rightarrow$ uniform (Cameron Thm 9)	✓ proven
`separation_dichotomy`	separate, *or* $\lvert gA \cap B\rvert{=}1$ $\forall g$ on one $\lvert A\rvert\lvert B\rvert$-orbit	✓ proven
`..._eq_one_iff_factorization`	extremal $\iff$ exact factorization $G = B \cdot A^{-1}$	✓ proven
`..._vadd_inter_eq_one_iff_tiling`	over $\mathbb{Z}/n$: extremal $\iff$ rhythmic tiling canon	✓ proven
`distinguishingNumber` (+API)	least k with a symmetry-killing k-colouring	• defined
`distinguishingNumber_le_card_base...`	base of size $b \Rightarrow D \le b{+}1$ (bridge to IBIS)	✓ proven
`fano_distinguishingNumber`	$D(\mathrm{GL}_3(\mathbb{F}_2) \curvearrowright \mathbb{F}_2^3) = 4$	✓ proven
IBIS (Cameron–Fon-Der-Flaass)	irredundant bases const. size $\iff$ matroid	○ future
bridge lemmas	separation $\leftarrow$ engine; extremal = Thm 8 $\ell{=}1$	○ future
Chan full classification	the $D{=}3$ cases; general $D{=}2$; PGL analogue	○ future

References

[1] B. J. Birch, R. G. Burns, S. Oates Macdonald, P. M. Neumann, *On the orbit-sizes of permutation groups containing elements separating finite subsets*, Bull. Austral. Math. Soc. **14** (1976) 7–10.

[2] B. H. Neumann, *Groups covered by permutable subsets*, J. London Math. Soc. **29** (1954) 236–248.

[3] J. Araújo, P. J. Cameron, B. Steinberg, *Between primitive and 2-transitive: synchronization and its friends*, EMS Surv. Math. Sci. **4** (2017) 101–184.

[4] P. J. Cameron, *Synchronization*, lecture notes (LTCC), 2010; `https://cameroncounts.wordpress.com/lecture-notes/`.

[5] M. Barbieri, P. Lekše, P. Potočnik, K. Rekvényi, *Separating subsets from their images* (2025), arXiv:2508.20731.

[6] P. J. Cameron, D. G. Fon-Der-Flaass, *Bases for permutation groups and matroids*, European J. Combin. **16** (1995) 537–544.

[7] M. O. Albertson, K. L. Collins, *Symmetry breaking in graphs*, Electron. J. Combin. **3** (1996) #R18.

[8] J. Tymoczko, *Distinguishing numbers for graphs and groups*, Electron. J. Combin. **11** (2004) #R63.

[9] M. Chan, *The maximum distinguishing number of a group*, Electron. J. Combin. **13** (2006) #R70.

[10] S. Klavžar, T.-L. Wong, X. Zhu, *Distinguishing labelings of group action on vector spaces and graphs*, J. Algebra **303** (2006) 626–641.

[11] E. M. Coven, A. Meyerowitz, *Tiling the integers with translates of one finite set*, J. Algebra **212** (1999) 161–174.

[12] D. T. Vuza, *Supplementary sets and regular complementary unending canons (Parts One–Four)*, Perspectives of New Music **29**(2) (1991), **30**(1),(2) (1992), **31**(1) (1993).

[13] B. Fuglede, *Commutative sets of self-adjoint partial differential operators and the group of orthogonal exponentials*, J. Funct. Anal. **16** (1974) 101–121.

[14] E. Amiot, *Music Through Fourier Space: Discrete Fourier Transform in Music Theory*, Springer, 2016.

[15] The mathlib Community, *The Lean mathematical library*, CPP 2020.