THE CHROMATIC NUMBER OF THE GRASSMANN GRAPH $J_2(6,3)$ LIES BETWEEN 19 AND 24, AND NO PUBLISHED REPRESENTATIVE OF A KNOWN APN CLASS ON $\mathbb{F}_{2^6}$ IS THIRD-ORDER SUM-FREE

KOREA SUPERINTELLIGENCE LABS

Abstract. A function $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ is *kth-order sum-free* if the sum of its values over every affine k-dimensional flat of $\mathbb{F}_2^n$ is nonzero; for $k=2$ this is almost perfect nonlinearity. Heering, Kaspers and Taranchuk showed that a $\{k-1,k\}$-order sum-free (n,m)-function of algebraic degree k yields a proper colouring of the Grassmann graph $J_2(n+1,k)$ with 2^m-1 colours, and obtained from the cubic function x^7 on $\mathbb{F}_{2^5}$ the bound $\chi(J_2(6,3)) \le 31$, the best known. We give a colouring of $J_2(6,3)$ with 24 colours: an explicit partition of the 1395 planes of $PG(5,2)$ into 24 constant-dimension subspace codes of minimum subspace distance 4, of sizes 51 to 76, all within the maximum $A_2(6,4;3)=77$ of Honold, Kiermaier and Kurz. Spending that same 77 in the ratio bound gives $\chi(J_2(6,3)) \ge 19$, so the published window $15 \le \chi(J_2(6,3)) \le 31$ becomes $19 \le \chi(J_2(6,3)) \le 24$; the exact value remains open, and the 24-colouring is a certificate found by search, not a construction, so it says nothing about $J_2(n,3)$ for other n. On the source paper's own open problem — do APN and third-order sum-free functions on $\mathbb{F}_{2^n}$ exist for $n>5$? — we verify their $n=5$ examples and settle the published 6-bit data: the six APN power maps, the six Kim-type maps, and the published representative of each of the 14 known CCZ-classes on $\mathbb{F}_{2^6}$ are all APN and none is third-order sum-free. This is not a nonexistence statement, and we say exactly why. Along the way the base-64 representative table we decoded is found to appear misaligned with its own invariant columns by five rows. Every theorem below is machine-checked in Lean 4.

1. Introduction

Sum-free functions. Let $n \ge 1$. A *k-flat* of $\mathbb{F}_2^n$ is a coset $A = U + a$ of a k-dimensional linear subspace $U \le \mathbb{F}_2^n$; it has 2^k points. For an (n,m)-function $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ and a flat A write

$$\omega_F(A) = \sum_{x\in A} F(x) \in \mathbb{F}_2^m.$$

Following Carlet, F is *kth-order sum-free* when $\omega_F(A) \ne 0$ for every k-flat $A \subseteq \mathbb{F}_2^n$ [8]. An (n,n)-function is *almost perfect nonlinear* (APN) when $F(x+a)+F(x)=b$ has at most two solutions x for every $a \ne 0$ and every b, and it is classical [10, 3] that APN is exactly second-order sum-freeness; so kth-order sum-freeness for $k \ge 3$ is a strengthening of a much-studied cryptographic condition, and a function that is $\{2,3\}$-order sum-free is fighting on two adjacent fronts at once.

The source of everything below is the paper of Heering, Kaspers and Taranchuk [8], which relates sum-free functions to Reed–Muller subcodes and to partitions of Grassmannians. Two of its results and two of its open questions are what this paper is about. The first is their second open problem:

Problem 1.1 ([8, Problem 7.2])**.** Do there exist functions in $\mathbb{F}_{2^n}$ that are APN and third-order sum-free for $n>5$? If yes, is this true for infinitely many values of n?

They record that on $\mathbb{F}_{2^5}$ the functions x^7, x^{21} (cubic) and the inverse function x^{30} are third-order sum-free, and that among the seven EA-classes of APN functions on $\mathbb{F}_{2^5}$ no others are; and that for $n=6$, over the 716 EA-classes of the known classification, their own computation finds none that is third- or fourth-order sum-free. The smallest open case of Problem 1.1 is $n=6$.

The Grassmann graph. The Grassmann graph $J_2(n,k)$ has as vertices the k-dimensional linear subspaces of $\mathbb{F}_2^n$, two of them adjacent when they meet in a $(k-1)$-space. Writing $d_S(U,W) = \dim U + \dim W - 2\dim(U\cap W)$ for the subspace distance, a set of k-spaces is independent in $J_2(n,k)$

exactly when it is a constant-dimension subspace code of minimum subspace distance at least 4; so a proper colouring of $J_2(n,k)$ with c colours is exactly a partition of the Grassmannian into c such codes, and $\chi(J_2(n,k))$ measures how many are needed [8, §2.3]. The best known general bounds for $q=2$ are

$$\max\left\{ \begin{bmatrix} k+1 \\ 1 \end{bmatrix}_2, \begin{bmatrix} n-k+1 \\ 1 \end{bmatrix}_2 \right\} \;\le\; \chi(J_2(n,k)) \;\le\; \begin{bmatrix} n \\ 1 \end{bmatrix}_2,$$

the upper bound from D'haeseleer and Taranchuk [5, Thm. 1.2], the lower bound from D'haeseleer, Pavese, Santonastaso and Taranchuk [6, Prop. 3.1]; see [8, Prop. 2.15], where both are collected. At $n=6$, $k=3$ the two Gaussian binomials in the maximum are both $\left[\begin{smallmatrix}4\\1\end{smallmatrix}\right]_2 = 15$, so the bounds read $15 \le \chi(J_2(6,3)) \le 63$.

The second result of [8] that concerns us is their colouring theorem [8, Thm. 5.1]: if there is an (n,m)-function F of algebraic degree k that is $\{k-1,k\}$-order sum-free, then $J_2(n+1,k)$ has a proper colouring with $\left[\begin{smallmatrix}m\\1\end{smallmatrix}\right]_2 = 2^m-1$ colours, given explicitly as follows. Identify $\mathbb{F}_2^{n+1}$ with $\mathbb{F}_2^n \times \mathbb{F}_2$, let $H = \mathbb{F}_2^n \times \{0\}$ be the resulting hyperplane, and for a set $S \subseteq \mathbb{F}_2^{n+1}$ put $\Omega_F(S) = \sum_{(v,\varepsilon)\in S} F(v) \in \mathbb{F}_2^m$. Then, by their Definition 5.4, the colour of a k-space $U \le \mathbb{F}_2^{n+1}$ is

$$c_F(U) = \begin{cases} \Omega_F(U) & \text{if } U \subseteq H, \\ \Omega_F(U \setminus H) & \text{if } U \not\subseteq H. \end{cases} \tag{1}$$

(When $U \not\subseteq H$ the set $U \cap H$ is a hyperplane of U, so $U \setminus H$ is a $(k-1)$-flat and has 2^{k-1} points.) Instantiated at $n=5$, $k=3$, $m=5$ with $F=x^7$ — which is cubic and $\{2,3\}$-order sum-free — this gives their Corollary 6.2, $\chi(J_2(6,3)) \le 31$, which they state "improves the previously best known upper bounds" [8, §1] of [5, 6]. It is the record: 31 against a general bound of 63. So the published window on the chromatic number of this one 1395-vertex graph is

$$15 \;\le\; \chi(J_2(6,3)) \;\le\; 31. \tag{2}$$

What is settled here. We narrow (2) from both sides, and we settle what the published 6-bit APN data can say about Problem 1.1.

The main result is an explicit colouring.

Theorem 1.2. $\chi(J_2(6,3)) \le 24$. *Explicitly, the* 1395 *planes of* $PG(5,2)$ *— the* 3*-dimensional subspaces of* $\mathbb{F}_2^6$ *— are covered by* 24 *classes, no one of which contains two distinct spaces meeting in a* 2*-space; equivalently, by* 24 *constant-dimension subspace codes with* $v=6$, $k=3$ *and minimum subspace distance* 4.

The 24 classes turn out to be pairwise disjoint, so the cover is a partition, and their sizes are

76, 75, 64, 63, 63, 60, 59, 59, 58, 58, 57, 57, 57, 56, 56, 55, 55, 54, 54, 53, 52, 52, 51, 51,

summing to 1395 and all at most the maximum $A_2(6,4;3) = 77$ (Proposition 4.2).

Against this, the same 77 bounds the classes from below in number.

Proposition 1.3. *Suppose every set of* 3*-spaces of* $\mathbb{F}_2^6$ *that is pairwise at subspace distance at least* 4 *has at most* 77 *members — the theorem* $A_2(6,4;3) = 77$ *of Honold, Kiermaier and Kurz* [9]*, used here as a hypothesis and not reproved. Then no family of fewer than* 19 *such sets covers the* 1395 3*-spaces of* $\mathbb{F}_2^6$*; that is,* $\chi(J_2(6,3)) \ge 19$.

Proposition 1.3 is a ratio bound and is one line of arithmetic on top of two published numbers: $77 \cdot 18 = 1386 < 1395$. We do not claim it as new mathematics; we record it because it is what makes the window two-sided, and because we have not found it written down — the lower bound quoted in this literature is the clique bound 15, which counts the 15 3-spaces through a fixed 2-space. Together with Theorem 1.2:

$$19 \;\le\; \chi(J_2(6,3)) \;\le\; 24. \tag{3}$$

On the APN side, §6 records what the published 6-bit data gives. Every one of the six APN power maps and six Kim-type maps on $\mathbb{F}_{2^6}$, and the published representative of each of the 14 known

CCZ-classes, is APN and is not third-order sum-free (Theorems 6.2 and 6.3). These are verifications, not new mathematics: the class-level negative over all 716 EA-classes is the computation of [8] itself. What we add is that the published representatives are checked from their published tables in a proof assistant, that the decoding of those tables is audited three independent ways, and that the audit turns up a transcription hazard in the source table (Remark 6.5).

What is not settled. Four disclaimers, all load-bearing.

The value of $\chi(J_2(6,3))$ *is not determined.* Theorem 1.2 is a certificate found by heuristic search; 24 is not claimed optimal. A 23-colouring is not excluded by counting — it needs an average class of 60.7 against a maximum of 77 — and was not found; §4 says what was spent.

Theorem 1.2 is not a construction. It is a table of 1395 records. It therefore says nothing about $\chi(J_2(n,3))$ for $n \neq 6$, and in particular does not compete with the general bounds of [5, 6], which it beats only at this one point.

Problem 1.1 stays exactly as open as it was. Third-order sum-freeness is invariant under degree-2 equivalence but *not* under CCZ-equivalence, so 14 representatives do not cover the 716 EA-classes they represent; and the completeness of the 14-class list is itself an open conjecture. "Every known class representative fails" is not "no APN function on $\mathbb{F}_{2^6}$ is third-order sum-free".

$A_2(6,4;3) = 77$ *is not proved here.* Proposition 1.3 carries it as an explicit hypothesis and spends it; the citation is [9].

2. Preliminaries

Throughout, a point of $\mathbb{F}_2^n$ is identified with its bit vector read as an integer in $[0, 2^n)$, and vector addition is bitwise exclusive-or; this identification involves no choice. The Gaussian binomial $\begin{bmatrix} n \\ k \end{bmatrix}_2$ counts the k-dimensional subspaces of $\mathbb{F}_2^n$. We use

$$\begin{bmatrix} 6 \\ 3 \end{bmatrix}_2 = 1395, \qquad \begin{bmatrix} 5 \\ 3 \end{bmatrix}_2 = 155, \qquad \begin{bmatrix} 6 \\ 1 \end{bmatrix}_2 = 63, \qquad \begin{bmatrix} 4 \\ 1 \end{bmatrix}_2 = 15, \qquad \begin{bmatrix} 3 \\ 2 \end{bmatrix}_2 = 7.$$

Flats and sum-freeness. A 3-flat of $\mathbb{F}_2^n$ is a coset of a 3-dimensional subspace, so an 8-point set $\{x, x+a, x+b, x+c, x+a+b, x+a+c, x+b+c, x+a+b+c\}$ with a, b, c linearly independent. On $\mathbb{F}_2^6$ there are 1395 such subspaces and hence $1395 \cdot 8 = 11{,}160$ flats; on $\mathbb{F}_2^5$ there are 155 subspaces and 620 flats. We quantify over ordered independent triples (a, b, c) together with a base point x; since $|GL_3(\mathbb{F}_2)| = 168$, each subspace is met exactly 168 times, and

$$63 \cdot 62 \cdot 60 = 234{,}360 = 168 \cdot 1395, \qquad 31 \cdot 30 \cdot 28 = 26{,}040 = 168 \cdot 155,$$

so the quantifier ranges over exactly the flats it should. These two identities are checked rather than assumed (Proposition 6.4).

Algebraic degree. The algebraic degree of an (n, m)-function is the largest degree of a monomial in its coordinate functions' algebraic normal forms. We use one classical fact, [8, Prop. 2.4]: $\omega_F(A) = 0$ for every k-flat A if and only if $\deg(F) \le k-1$. In particular a quadratic function sums to zero over *every* 3-flat and is as far from third-order sum-free as possible, and a kth-order sum-free function has degree at least k.

The two fields. Power maps and Kim-type maps are defined through a finite field, though neither APN-ness nor sum-freeness refers to the multiplication. We realise $\mathbb{F}_{2^6}$ as $\mathbb{F}_2[x]/(x^6 + x^4 + x^3 + x + 1)$ (the Conway polynomial, so tables agree with the usual computer algebra conventions) and $\mathbb{F}_{2^5}$ as $\mathbb{F}_2[x]/(x^5 + x^2 + 1)$. Any other irreducible modulus conjugates every map by a field isomorphism, which is $\mathbb{F}_2$-linear and so preserves both properties. The field axioms and the primitivity of x are verified for both realisations.

The Grassmann graph $J_2(6,3)$. Its vertices are the 1395 3-spaces of $\mathbb{F}_2^6$, equivalently the planes of $PG(5,2)$; two are adjacent when they meet in a 2-dimensional subspace, i.e. in a line of $PG(5,2)$. Each 3-space contains $\begin{bmatrix} 3 \\ 2 \end{bmatrix}_2 = 7$ two-dimensional subspaces, each of which lies in $\begin{bmatrix} 4 \\ 1 \end{bmatrix}_2 - 1 = 14$ further 3-spaces, so the graph is $7 \cdot 14 = 98$-regular and has $1395 \cdot 98/2 = 68{,}355$ edges out of $\binom{1395}{2} = 972{,}315$ pairs. For distinct 3-spaces U, W one has $\dim(U \cap W) \le 2$, so $d_S(U, W) = 6 - 2\dim(U \cap W) \in \{2, 4, 6\}$;

hence a set of 3-spaces is independent in $J_2(6,3)$ exactly when no two of its members meet in a 2-space, exactly when it is a constant-dimension subspace code with $v=6$, $k=3$, $d=4$. The maximum size of such a code is $A_2(6,4;3)=77$ [9].

The computational model. A 3-space is represented by the 64-bit incidence mask of its eight points, so intersection is bitwise AND and $\dim(U\cap W)=2$ is $\operatorname{popcount}(m_U\wedge m_W)=4$; two equal spaces meet in eight points, so the adjacency test is automatically irreflexive. The vertex list is produced by filtering ordered triples (a,b,c) by independence together with a canonicality predicate (a least nonzero point of the span, b least point outside $\{0,a\}$, c least point outside the plane $\{0,a,b,a+b\}$). That this enumerates each 3-space exactly once is not assumed; it is pinned from three sides in Proposition 3.1 below.

3. The model, and the published 31-colouring

Before improving a published bound we reproduce it, from the source's own definitions, in the same terms in which the new bound will be stated.

Proposition 3.1. *The list of* 3*-spaces described in §2 has exactly* 1395 *entries, its masks are pairwise distinct, and the span of* every *ordered independent triple of points of* $\mathbb{F}_2^6$ *occurs on it; so it is exactly the vertex set of* $J_2(6,3)$*. With the adjacency test above, every vertex has exactly* 98 *neighbours and the degree sum is* $2\cdot 68{,}355$*. Moreover, for* $F=x^7$ *and for* $F=x^{21}$ *on* $\mathbb{F}_{2^5}$*, the colouring* c_F *of* (1) *uses exactly* 31 *colours, gives the forbidden colour* 0 *to no vertex, and has no monochromatic edge. In particular the* 31 *colour classes of* c_{x^7} *cover all* 1395 3*-spaces and none of them contains two distinct spaces meeting in a* 2*-space:* $\chi(J_2(6,3))\le 31$.

The last sentence is Corollary 6.2 of [8]; the content added here is that it is verified from their Definition 5.4, reproduced as (1), against a graph model that has itself been pinned down.

Proof sketch. Everything is a finite check, and each is exhaustive over its stated range. The count and the distinctness are read off the 1395-entry list. Completeness is the check that for all $64^3=262{,}144$ ordered triples (a,b,c) — of which 234,360 are independent — the span of an independent triple appears on the list; this is what makes "covers" below mean covers, since it says the list omits no 3-space. Regularity is 1395 degree computations, each a sweep over the 1395 vertices. For the colourings, c_F is evaluated at all 1395 vertices from the value table of F on $\mathbb{F}_{2^5}$, and the number of monochromatic ordered adjacent pairs is computed by a full 1395×1395 sweep. The value tables of x^7 and x^{21} are themselves obtained from the field arithmetic and checked against independently generated tables at all 32 points. $\square$

The hypotheses of the source's colouring theorem are not decoration, and the same graph shows it. Recall that x^{30}, the inverse function on $\mathbb{F}_{2^5}$, is $\{1,2,3,4\}$-order sum-free — hence $\{2,3\}$-order sum-free — but has algebraic degree 4, not 3; and that x^3 and x^5 are quadratic Gold maps, APN and hence second-order sum-free, but of degree 2 and so not third-order sum-free at all.

Proposition 3.2. *Applied to* x^{30}*, the construction* (1) *gives no vertex the colour* 0 *but produces* 310 *monochromatic edges. Applied to* x^3 *and to* x^5 *it gives the forbidden colour* 0 *to exactly* 155 *of the* 1395 *vertices; for* x^3 *it moreover produces* 7595 *monochromatic edges. The adjacency relation is neither empty nor complete:* $0<68{,}355<972{,}315$.

The number 155 is not "some failures". It is $\left[\begin{smallmatrix}5\\3\end{smallmatrix}\right]_2$, the number of 3-spaces contained in the hyperplane H, which is exactly the predicted failure set: on $U\subseteq H$ the definition (1) returns $\omega_F(U)$, and a function of algebraic degree at most 2 sums to zero over every 3-flat. So the degree hypothesis fails in one place and the sum-freeness hypothesis in another, each visibly where the source's proof uses it.

4. A colouring with 24 colours

The certificate. The colouring of Theorem 1.2 is carried as data: 1395 records, one per 3-space, each giving the canonical basis (a,b,c) of the space and its colour in $[0,24)$, packed as eight hexadecimal digits. Nothing about the way the data was found enters the proof. What is proved about it is the following list of exhaustive finite checks.

Proposition 4.1. *Let R be the table of 1395 records and let $C_0, \dots, C_{23}$ be the sets of spans it induces. Then: each of the 1395 recorded triples is linearly independent, so each recorded object is a 3-space; the 1395 spans are pairwise distinct; every recorded colour is < 24, and there are 24 classes; every 3-space of $\mathbb{F}_2^6$ lies in some C_i; and no C_i contains two distinct spaces meeting in a 2-space.*

Proof sketch of Proposition 4.1 and Theorem 1.2. Five checks, each exhaustive over the range stated. (i) Independence: 1395 tests, one per record. (ii) Distinctness: each of the 1395 masks is counted in the list of 1395 masks and found exactly once. (iii) Colour range and class count: 1395 comparisons and one length. (iv) Cover: for each of the 1395 vertices of the model of §3 — which by Proposition 3.1 really is the set of *all* 3-spaces of $\mathbb{F}_2^6$, so that this is a genuine cover of the Grassmannian and not of a sublist — membership in some C_i is checked. (v) Cocliqueness: within each class, all ordered pairs (m, m') are tested for $\mathrm{popcount}(m \wedge m') = 4$, about $\sum_i |C_i|^2 \approx 8.2 \times 10^4$ tests in total. Since $\sum_i |C_i| = 1395$ and the spans are distinct, the classes are disjoint and the cover is a partition. Combining (iii), (iv), (v) with the completeness clause of Proposition 3.1 gives Theorem 1.2; the class sizes are read off in one further computation. The correctness of the conclusion depends on these checks alone, not on the search of §4. □

Proposition 4.2. *The 24 classes are nonempty, pairwise disjoint, and sum to 1395, so the data is not a 23-colouring with one class split in two. Deleting any one class leaves 3-spaces uncovered, so this data does not contain a 23-colouring. Each of the $\binom{24}{2} = 276$ pairs of classes has an edge between them, so no two classes may be merged. Every class has at most 77 members, the largest having 76. Finally, the property "pairwise at subspace distance at least 4" is neither vacuously true nor vacuously false on this model: the full vertex set does not have it, and the first class does.*

The bound $76 \le 77$ is worth pausing on. It is an external consistency check on the whole model: an adjacency test that was too weak would admit a class larger than the published maximum $A_2(6, 4; 3) = 77$, and with a class of 76 there is exactly one unit of slack left.

How the colouring was found, and what was not found. The colouring is the output of a search, and the search is not exhaustive; only its output is verified. All runs were single-threaded on the 1395-vertex graph generated by an independent implementation of the model of §2.

method	best reached	measured cost
random-restart tabu colouring	25	≈6 CPU-min
warm-started tabu, drop-smallest-class restarts	25; 24 not found in 24 runs of $8 \cdot 10^6$ iterations	≈45 CPU-min
greedy cover: peel a large independent set, delete, repeat	28	≈4 CPU-min
tabu colouring seeded by that greedy cover	25, then **24**	≈6 CPU-min
local search for a single maximum independent set	71 (true maximum 77)	≈8 CPU-min

The lesson is the seeding rather than the budget: tabu colouring from random and from drop-smallest restarts did not reach 24 in $24 \times 8 \cdot 10^6$ iterations, and a warm start from the greedy cover reached it in about four CPU-minutes. The greedy cover's profile — a dozen classes near the maximum size and a short tail — is what the local search can repair; a balanced 25-colouring is not. Total search cost was about 1.5 CPU-hours.

A 23-colouring was not reached. The run that produced 24 was continued at 23 for a further ≈15 CPU-minutes without success and then stopped. Nothing follows from this beyond Proposition 4.2: the 24 classes at hand cannot be merged or dropped into 23.

Remark 4.3 (outside the formal development). A colouring with c classes all of the same size needs $c \mid 1395 = 3^2 \cdot 5 \cdot 31$. The divisors of 1395 that are less than 31 are $1, 3, 5, 9, 15$, and already $1395/15 =$

$93 > 77 = A_2(6,4;3)$. So 31 is the largest number of colours for which a balanced colouring can exist, which explains why the published 31 has the shape it has, and every improvement on it must be unbalanced. Both the 25-colourings found above and the 24-colouring of Theorem 1.2 are unbalanced, with sizes spanning 51 to 76. This remark is arithmetic commentary; it is not part of the formal development.

5. The lower end, and the window

Proof sketch of Proposition 1.3. A colour class is a set of 3-spaces pairwise at subspace distance at least 4, i.e. a set of planes of $PG(5,2)$ meeting pairwise in at most a point. If every such set has at most 77 members and c of them cover the 1395 3-spaces, then $1395 \le 77c$, so $c \ge 1395/77 > 18$, i.e. $c \ge 19$. Formally: the vertex list is duplicate-free, so a cover is a sublist-permutation of the concatenation of the classes, whence $1395 \le \sum_i |C_i| \le 77c$. The only finite computations entering this argument are the vertex count 1395 and the duplicate-freeness of the vertex list; the rest is arithmetic. The margin is exactly $77 \cdot 18 = 1386 < 1395 \le 1463 = 77 \cdot 19$. □

Combining with Theorem 1.2 gives (3): there exist 24 classes that cover $J_2(6,3)$, and — given $A_2(6,4;3) = 77$ — no 18 classes do. Both halves are stated in the same terms, so the two records are directly comparable, and the window $19 \le \chi(J_2(6,3)) \le 24$ replaces the published $15 \le \chi(J_2(6,3)) \le 31$.

We did not exhibit an independent set of size 77; the largest found by a standalone search was 71, and the largest class of Theorem 1.2 has 76. Nothing above uses the existence of a 77-set, only the nonexistence of a 78-set.

What the novelty of Theorem 1.2 rests on. The bound it improves is three months old and, as far as we can determine, unimproved and uncited. The searches actually run, on 30 August 2026, were: a local full-text arXiv corpus of 881,145 papers covering announcements through 28 August 2026, queried for the patterns `chromatic number of.{0,30}Grassmann`, `J_2(6,3)`, `A_2(6,4;3)`, `2-parallelism`, `1395 planes`, `sum-free function` and the authors' names; the live arXiv API, which reports [8] as v1 only; and Semantic Scholar, which reports zero citations of it. No paper in that corpus mentions $\chi(J_2(6,\cdot))$ at all outside [8]. The two general bounds that [8] names as the previous records [8, §1] give 63 and 48 here. The first is $\chi(J_2(6,3)) \le \left[{6 \atop 1}\right]_2 = 63$, immediate from [5, Thm. 1.2]. The second is ours to instantiate and is not a number printed in [6]: their Theorem 4.7 states $\chi(J_q(n,m,t)) \le \chi(J(n,m,t))\, q^{(n-m)(m-t)}$ for $n \ge 2m$, where $J(n,m,t)$ is the $(m-t)$th power of the Johnson graph $J(n,m)$; at $q=2$, $n=6$, $m=3$, $t=2$ we have $n=2m$, the power is the first, so $J(6,3,2) = J(6,3)$, and $q^{(n-m)(m-t)} = 2^3 = 8$, while the classical bound $\chi(J(n,m)) \le n$ that [6, §1] quotes from Graham and Sloane gives $\chi(J(6,3)) \le 6$; together, $\chi(J_2(6,3)) \le 6 \cdot 8 = 48$. Neither paper tabulates small cases and neither writes either number. The classical literature on plane parallelisms of $PG(5,2)$ — equivalently, on resolutions of the 2-$(63,7,15)$ design of the points and planes, classified under various group hypotheses by Sarmiento [12] and by Topalova and Zhelezova [13] — partitions the same 1395 planes into 155 *spreads* of 9 mutually disjoint planes each. That is a strictly stronger and much smaller kind of class, and so gives only $\chi \le 155$; it is not a competitor.

6. APN and third-order sum-free functions on $\mathbb{F}_{2^6}$

We turn to Problem 1.1. The results of this section are verifications of published objects and published data; none of them is claimed as new mathematics. Their point is that they are checked, in the kernel of a proof assistant, from the published tables, with an audit trail for the decoding of those tables.

Proposition 6.1. *On $\mathbb{F}_{2^5}$ the power maps x^7, x^{21} and x^{30} are each APN and third-order sum-free. In particular there exists a function on $\mathbb{F}_{2^5}$ that is APN and third-order sum-free.*

These are the examples of [8]; the statement is theirs, the verification ours. The positive half is the expensive direction: third-order sum-freeness on $\mathbb{F}_{2^5}$ is a scan over all 32^4 tuples (a,b,c,x), whose

26,040 independent triples times 32 base points cover each of the 620 flats $168 \cdot 8$ times. Proposition 6.1 is also the reason to believe the checkers can say *yes*: no function on $\mathbb{F}_{2^6}$ below ever makes them do so.

Theorem 6.2. *The six APN power maps on $\mathbb{F}_{2^6}$ — $x^3, x^6, x^{12}, x^{24}, x^{33}, x^{48}$, whose exponents are exactly the cyclotomic coset $\{3 \cdot 2^i \bmod 63\}$ of the Gold exponent 3 — and the six Kim-type maps $x^3 + x^{10} + u\,x^{24}$ with $u \in \{2, 4, 16, 19, 50, 55\}$ are each APN, and none of them is third-order sum-free.*

Theorem 6.3. *The published representative of each of the 14 known CCZ-equivalence classes of APN functions on $\mathbb{F}_{2^6}$, as tabulated in the "Code-64" table of Gillot and Langevin [7], is APN and is not third-order sum-free.*

Proof sketch of Theorems 6.2 and 6.3. Each map is first proved equal, at all 64 points, to an explicit value table generated by an independent implementation of the same field arithmetic; the property checks then run on the table. The APN half is an exhaustive scan over all (a, b) with $a \neq 0$, counting solutions of $F(x + a) + F(x) = b$; for the 14 representatives this scan is also the validation of the decoding, since the base-64 packing convention is pinned by being the unique one of the three plausible ones under which all 14 tables come out APN. The negative half is a single witness in each case: an explicit independent triple (a, b, c) and base point x over which the eight values sum to zero. Twelve of the fourteen representatives and all twelve classical maps are quadratic, so every one of the 11,160 flats witnesses the failure and the witness $\langle 1, 2, 4\rangle + 0$ serves for all of them; the two cubic representatives fail on 2456 and 3992 flats respectively, with witnesses $\langle 1, 2, 8\rangle + 0$ and $\langle 1, 2, 32\rangle + 0$. Because each negative is a single witness rather than a search, its verification needs no evaluation axiom at all: these statements are checked by the kernel outright, with propositional extensionality as the only axiom. □

Proposition 6.4. *The APN test rejects the identity map on $\mathbb{F}_{2^6}$ and the power maps x^5 and x^7 on $\mathbb{F}_{2^6}$. The third-order sum-freeness test rejects the zero map — so the independence predicate is satisfiable and the quantifier is not vacuous — and rejects the table of the genuine example x^7 on $\mathbb{F}_{2^5}$ with one entry altered, which fails on only 5 of the 620 flats; over all $32 \cdot 31$ single-entry perturbations of that table, 5 is the minimum number of vanishing flats, so no one-entry miss is nearer. The number of ordered independent triples is $234{,}360 = 168 \cdot 1395$ on $\mathbb{F}_{2^6}$ and $26{,}040 = 168 \cdot 155$ on $\mathbb{F}_{2^5}$, tying the quantifier's range to the subspace counts of* [8].

What this does and does not say about Problem 1.1. The known APN functions on $\mathbb{F}_{2^6}$ are classified up to EA-equivalence by Calderini [4]; as reported in [8, §6] they fall into 14 CCZ-classes and 716 EA-classes, of which 521 are cubic and 182 have algebraic degree 4, and that list is conjectured complete [1]. Theorem 6.3 covers one representative of each CCZ-class. It does not cover the 716 EA-classes, because third-order sum-freeness is invariant under degree-2 equivalence but not under CCZ-equivalence: a CCZ-class may contain both sum-free and non-sum-free functions as far as anything proved here is concerned. The EA-exhaustive negative is the computation reported in [8], which we did not reproduce — the lists of the 703 representatives of degree at least 3 that it ran on were not available to us. And even the EA-exhaustive negative is not a nonexistence theorem, since completeness of the classification is open. So the citable consequence is exactly: *the $n = 5$ examples verify, and no published representative of a known 6-bit APN class answers Problem 1.1* — nothing stronger.

Remark 6.5 (a transcription hazard, outside the formal development). In Table 2 of [7] the "Code-64" column appears to be misaligned with the Γ-rank and degree-distribution columns beside it by five rows, cyclically. We state this as an observation about one version of one table, checked on 30 August 2026 against arXiv:2601.11247v1 — at that date the only version — and against nothing else; we have not contacted the authors, and no claim about the underlying mathematics is intended. The evidence is threefold. First, the Γ-rank of the table decoded from printed row k equals the Γ-rank printed at row $k + 5 \bmod 14$, in all 14 rows. Second, the unique class with no quadratic member — printed with degree distribution 0/10/15 and Γ-rank 1300 at row 6 — is the table decoded from row 1, which is indeed cubic of Γ-rank 1300. Third, an independent alignment against the per-class vanishing-3-subspace multisets of [8]: our decoded row 1 has 307 vanishing 3-subspaces and decoded row 4 has 499, and each of those values occurs in exactly one row of their table, whose degree distributions are then those printed at rows 6 and 9 of [7] — the same five-row shift. (That table of [8] is present in its arXiv source but suppressed from the article, so it is evidence available to us rather than published evidence.) For a cubic function the third derivative is constant, so a vanishing subspace vanishes on all eight of its cosets; and indeed $2456 = 8 \cdot 307$ and $3992 = 8 \cdot 499$. Theorem 6.3 and the statements around it are immune, since they treat the 14 tables as an unlabelled set of functions; but anyone citing "class k" by those printed labels should check first. This remark records a computation performed outside the formal development.

7. Verification

Every theorem and proposition above is formally verified in Lean 4 [11]; the development contains no `sorry` and no hand-written axiom. The graph model, the 24-colouring certificate and their controls are written against Lean's built-in prelude alone, without *Mathlib*, so that the statements are equations between natural numbers, lists and booleans and the checks fit in about 1.6 GB; the sum-free and APN definitions and the ratio bound of Proposition 1.3 are stated over *Mathlib*. The finite scans — the vertex enumeration and its completeness, the degree and edge counts, the evaluations of c_F, the five checks of Proposition 4.1, the controls, the APN scans and the positive sum-freeness scans of Proposition 6.1 — are delegated to compiled evaluation, and the axiom footprint of each such statement is the standard axioms of the ambient library (propositional extensionality, quotient soundness, and, for the statements phrased over finite types, the axiom of choice) together with the single evaluation axiom generated for it. Every negative sum-freeness statement in §6 is instead a single witness flat checked by the kernel outright, whose only axiom is propositional extensionality; the arithmetic of Proposition 1.3 is likewise kernel reasoning, its only evaluated inputs being the vertex count 1395 and the duplicate-freeness of the vertex list, and the margin $77 \cdot 18 = 1386 < 1395 \leq 77 \cdot 19$ carries no axiom at all. Every table and every count quoted here was produced first by an independent implementation in Python or C and only then stated and checked formally, so the formal run re-checks a known answer rather than searching for one. The development lives in a repository that is private at the time of writing; a public archival identifier for it — a public commit hash or a Zenodo DOI — is to be inserted here at submission.

8. What is open

The value of $\chi(J_2(6,3))$. Six values remain: $19, 20, 21, 22, 23, 24$. A 23-colouring is not excluded by the ratio bound and was not found; a serious attempt should be priced at at least 4 CPU-hours and should use a hybrid evolutionary colouring with partition crossover, seeded by several independent greedy covers, rather than more of the same tabu search. On the other side, the ratio bound is the only lower-bound argument used here; a bound using the structure of large subspace codes rather than only their size would be the first place to look for 20.

Problem 1.1. Untouched. Two concrete routes are visible and both are blocked on data rather than on ideas: the EA-exhaustive negative for $n = 6$ needs the lists of the 703 representatives of degree at least 3 that [8] ran on, after which each is one cheap witness check; the $n = 7$ analogue needs the corresponding lists. The positive direction — an APN function on $\mathbb{F}_{2^6}$ outside the known classes — is a search over 64^{64} maps with no known structure to exploit, and is precisely the object whose nonexistence is conjectured in [7, 1].

Other small cases. Theorem 1.2 is a single point. The same search-plus-certificate route applies verbatim to $J_2(7,3)$ (11,811 vertices) and to $J_2(6,2)$ and $J_2(7,2)$, where the published bounds again come from general theorems. We have not run it.

References

[1] J. Baudrin, P. Galissant and L. Perrin, *Exploring the Set of APN Functions*, BFA 2025 — 10th International Workshop on Boolean Functions and their Applications, Larnaca, Cyprus, 1–5 September 2025; preprint `hal-05376704`. The source of the conjecture that the known classification of APN functions on $\mathbb{F}_{2^6}$ is complete, and of the 716 EA-classes, as reported in [8, §6]; not consulted directly.

[2] D. Heinlein, M. Kiermaier, S. Kurz and A. Wassermann, *Tables of subspace codes*, arXiv:1601.02864v3 (2019); on-line database at `subspacecodes.uni-bayreuth.de`. Its entry for $q = 2$, $v = 6$, $d = 4$, $k = 3$ records lower bound 77 and upper bound 77.

[3] M. Brinkmann and G. Leander, *On the classification of APN functions up to dimension five*, Des. Codes Cryptogr. **49** (2008), no. 1–3, 273–288, doi:10.1007/s10623-008-9194-6. Cited by [8] for the classification of APN functions on $\mathbb{F}_{2^5}$ into seven EA-classes and, with [10], for the equivalence of APN with second-order sum-freeness; not consulted directly.

[4] M. Calderini, *On the EA-classes of known APN functions in small dimensions*, Cryptogr. Commun. **12** (2020), no. 5, 821–840, doi:10.1007/s12095-020-00427-1. The EA-classification of the known APN functions in dimension 6; the counts 14 and 716 are quoted here from [8, §6] and [7, §4]. Not consulted directly.

[5] J. D'haeseleer and V. Taranchuk, *On the Chromatic Number of Grassmann Graphs*, arXiv:2505.22055 (2025). Its Theorem 1.2 is the general bound $\begin{bmatrix} n-m+1 \\ 1 \end{bmatrix}_q \leq \chi(J_q(n,m)) \leq \begin{bmatrix} n \\ 1 \end{bmatrix}_q$, whose upper half gives 63 at $q = 2$, $n = 6$, $m = 3$.

[6] J. D'haeseleer, F. Pavese, P. Santonastaso and V. Taranchuk, *Chromatic Number of Grassmann Graphs and MRD codes*, arXiv:2602.10777 (2026). Its Proposition 3.1 is the lower bound restated in [8, Prop. 2.15], which gives 15 at $q = 2$, $n = 6$, $k = 3$; its Theorem 4.7 is the MRD lifting bound instantiated in §5.

[7] V. Gillot and P. Langevin, *On Known APNs*, arXiv:2601.11247v1 (2026); the article's own title page reads *Observation of known APNs*. Its Table 2 carries the "Code-64" representatives of the 14 known CCZ-classes of APN functions on $\mathbb{F}_{2^6}$ decoded for Theorem 6.3, and is the table discussed in Remark 6.5.

[8] P. Heering, C. Kaspers and V. Taranchuk, *On Reed-Muller subcodes, Grassmannian partitions and sum-free functions*, arXiv:2605.22958v1 (2026). All numbering, all quoted statements and Problem 1.1 are taken from that version, the only one at the time of writing; its results used here are the colouring theorem (their Theorem 5.1), the colouring function (1) (their Definition 5.4), the degree criterion (their Proposition 2.4), the collected general bounds (their Proposition 2.15), the Corollary $\chi(J_2(6,3)) \leq 31$ (their Corollary 6.2) and Problem 7.2.

[9] T. Honold, M. Kiermaier and S. Kurz, *Optimal Binary Subspace Codes of Length 6, Constant Dimension 3 and Minimum Distance 4*, arXiv:1311.0464v2; published as *Optimal binary subspace codes of length 6, constant dimension 3 and minimum subspace distance 4*, in: Topics in Finite Fields, Contemp. Math. **632**, Amer. Math. Soc., 2015, 157–176, doi:10.1090/conm/632/12627. The arXiv abstract states: "It is shown that the maximum size of a binary subspace code of packet length $v = 6$, minimum subspace distance $d = 4$, and constant dimension $k = 3$ is $M = 77$; in Finite Geometry terms, the maximum number of planes in PG(5, 2) mutually intersecting in at most a point is 77." This is the number carried as a hypothesis in Proposition 1.3 and used as an external check in Proposition 4.2. The value 77 was independently confirmed against the on-line tables of subspace codes maintained at Bayreuth, which record both bounds as 77 [2].

[10] X.-d. Hou, *Affinity of permutations of* $\mathbb{F}_2^n$, Discrete Appl. Math. **154** (2006), no. 2, 313–325, doi:10.1016/j.dam.2005.03.022. Cited by [8], with [3], for the equivalence of APN with second-order sum-freeness; not consulted directly.

[11] L. de Moura and S. Ullrich, *The Lean 4 theorem prover and programming language*, in: Automated Deduction — CADE 28, Lecture Notes in Computer Science 12699, Springer, 2021, 625–635, doi:10.1007/978-3-030-79876-5_37.

[12] J. F. Sarmiento, *On point-cyclic resolutions of the* 2-$(63, 7, 15)$ *design associated with* $PG(5, 2)$, Graphs Combin. **18** (2002), no. 3, 621–632, doi:10.1007/s003730200046. Not consulted directly.

[13] S. Topalova and S. Zhelezova, 2*-spreads and transitive and orthogonal* 2*-parallelisms of* $PG(5, 2)$, Graphs Combin. **26** (2010), no. 5, 727–735, doi:10.1007/s00373-010-0943-8. Not consulted directly.