DEGREE-THREE RELATIONS AMONG QUADRATIC FORMS: THE VALUE $\beta_2(7) = 16$, AND A CONJECTURED FAMILY PAST $n = 12$

KOREA SUPERINTELLIGENCE LABS

Abstract. Let $\mathbb{K}$ be a field of characteristic zero and let $q_1, \dots, q_m$ be quadratic forms in n variables over $\mathbb{K}$. In his work on uniqueness of powers-of-forms decompositions, Taveira Blomenhofer writes $\beta_2(n)$ for the largest m for which some such family admits no nonzero algebraic relation of degree at most three; the only bound he names is $\beta_2(n) \le \binom{n+1}{2}$, coming from linear relations, and he conjectures the lower bound $\beta_2(n) \ge \lceil (n+2)(n+1)/6 \rceil$, witnessed by the explicit family $q_{ijk} = (X_i + X_j + X_k)^2$ over the index triples $i \le j \le k$ with $i + j + k \equiv 0 \pmod n$, offering as evidence a computer verification for $n \in \{7, \dots, 12\}$. We determine $\beta_2(n)$ exactly for $2 \le n \le 7$. Counting the target space gives $\beta_2(n) \le \operatorname{mmax}(n) := \max\{m : \binom{m+2}{3} \le \binom{n+5}{6}\} \sim n^2/120^{1/3}$, sharper than the stated bound by a factor tending to $2.466\ldots$; and we exhibit $\operatorname{mmax}(n)$ explicit squares of linear forms with one-digit integer coefficients whose $\binom{\operatorname{mmax}(n)+2}{3}$ three-fold products are linearly independent, for $n = 4, 5, 6, 7$. The resulting values $\beta_2(n) = 7, 9, 13$ for $n = 4, 5, 6$ agree with what can be read off Table 1 of Friedman–Sturmfels–Wiesmann; $\beta_2(7) = 16$ lies past that table, and past the 12 that the conjectured family supplies, so that family is not optimal from $n = 4$ on. We also give what appears to be the first formal certificate for a case of the conjecture, at $n = 7$, where 364 products of 12 quadrics are shown independent over every field of characteristic zero; and we correct a remark of the source paper, whose asserted generator degree k^n for the relation ideal of $n + 1$ general k-forms in n variables has the exponent one too large — a degree count predicts k^{n-1}, which is what we measure at seven pairs (n, k). All independence statements rest on exhaustive finite computations, identified where they occur, and are machine-checked in Lean 4 with no `sorry`. Outside the formal development we record, as labelled computations, that the conjecture also holds at $n = 13, 14, 15, 16$ — $n = 13$ being the first case its source leaves open — and that $\beta_2(n) = \operatorname{mmax}(n)$ persists for $n = 8, \dots, 11$.

1. Introduction

The objects. Fix a field $\mathbb{K}$ of characteristic zero and write $S = \mathbb{K}[X_1, \dots, X_n]$ for the polynomial ring with its standard grading, so that $\dim_{\mathbb{K}} S_d = \binom{n+d-1}{d}$. For k-forms $q_1, \dots, q_m \in S_k$ let

$$\varphi_q \colon \mathbb{K}[Y_1, \dots, Y_m] \longrightarrow S, \qquad Y_a \mapsto q_a,$$

and let $I_{\mathrm{rel}}(q_1, \dots, q_m) := \ker \varphi_q$ be the *ideal of relations*. Since all q_a have the same degree, φ_q is graded up to the factor k and $I_{\mathrm{rel}}(q)$ is a homogeneous ideal; we write $I_{\mathrm{rel}}(q)_{\le 3}$ for the span of its elements of degree at most three. Following Taveira Blomenhofer [1], set

$$\beta_k(n) \;:=\; \max\big\{\, m \;:\; \text{there are } q_1, \dots, q_m \in S_k \text{ with } I_{\mathrm{rel}}(q_1, \dots, q_m)_{\le 3} = \{0\} \,\big\}.$$

Deleting a form from a family cannot create a relation, so the set of admissible m is an initial segment and $\beta_k(n)$ is well defined once it is finite; it is, by the bound $\beta_k(n) \le \binom{n+k-1}{k}$ from linear relations recalled below, and Proposition 3.1 sharpens that bound for $k = 2$. This paper is about $k = 2$: how many quadratic forms in n variables can avoid every relation of degree three?

Where the question comes from. The quantity $\beta_k(n)$ is introduced in [1], where the vanishing of $I_{\mathrm{rel}}(q)_{\le 3}$ is the first of two hypotheses under which a powers-of-forms decomposition is shown to be recoverable from a simple Gram spectrahedron. About β_2 that paper says three things. First, the only bound it names is the linear one, $\beta_k(n) \le \binom{n+k-1}{k}$, coming from relations of degree one, so $\beta_2(n) \le \binom{n+1}{2} \sim n^2/2$. Second, it credits $\beta_2(n) = \Theta(n^2)$ to Bafna–Hsieh–Kothari–Xu [3, §6.4],

adding "I am not aware of any other reference for this statement". Third, it proposes an explicit lower bound:

Conjecture 1.1 ([1, Conjecture 4.2])**.** The family

$$q_{ijk} := (X_i + X_j + X_k)^2, \qquad i \le j \le k, \quad i + j + k \equiv 0 \pmod{n},$$

of $m = \lceil (n+2)(n+1)/6 \rceil$ quadratics in n variables satisfies no algebraic relation of degree 3.

The evidence offered for it reads, in full: "Verified on a computer for $n \in \{7, \dots, 12\}$." Two questions are therefore open in the source. Does Conjecture 1.1 survive past $n = 12$? And what is $\beta_2(n)$ really — the conjectured family has size $\sim n^2/6$, the only recorded upper bound is $\sim n^2/2$, and nothing in [1] or in [3] narrows the gap.

What is settled here. We close the gap for small n, and in the process show that the conjectured family, whatever its fate, is not extremal.

Theorem 1.2 (Theorem 5.2, Proposition 3.1 and Corollary 5.3)**.** $\beta_2(7) = 16$. *Explicitly, there are* 16 *squares of linear forms in seven variables, with one-digit nonnegative integer coefficients, whose* $\binom{18}{3} = 816$ *three-fold products are linearly independent over every field of characteristic zero; and no* 17 *quadratic forms in seven variables avoid a relation of degree three.*

The number 16 is mmax(7), the largest m with $\binom{m+2}{3} \le \binom{12}{6}$, and it is 4 more than the 12 that Conjecture 1.1 supplies at $n = 7$. The same pair of bounds pins $\beta_2(n)$ for every $n \le 7$ (Corollary 5.3), the values being $4, 7, 9, 13, 16$ for $n = 3, 4, 5, 6, 7$; the first four of these already follow from Table 1 of Friedman–Sturmfels–Wiesmann [2], whose computations stop at six variables, and are recorded here with certificates rather than as new values (Theorem 5.1).

Theorem 1.3 (Theorem 6.1)**.** *Conjecture 1.1 holds at* $n = 7$*: the* $\binom{14}{3} = 364$ *three-fold products of the* 12 *quadrics* q_{ijk} *are linearly independent over every field of characteristic zero.*

The mathematical content of Theorem 1.3 is claimed in [1]; what is new is that it is here established by a method independent of the one used there — ranks of evaluation matrices modulo a prime, rather than of coefficient matrices — and that it is checked by a proof assistant, which as far as we know has not been done for any case of the conjecture.

Finally, Remark 4.3 of [1] asserts that for $m = n + 1$ general k-forms in n variables the relation ideal is principal, generated in degree k^n, and concludes $\beta_k(n) \ge n + 1$ for all $n \ge 2$, $k \ge 2$. The exponent is one too large: a degree count predicts k^{n-1}, and k^{n-1} is what we measure, at seven pairs (n, k) (§8). With the corrected exponent the conclusion is restored wherever $k^{n-1} > 3$, that is for all $n \ge 3$ and for $n = 2$ with $k \ge 4$; it fails at $(n, k) = (2, 2)$, where $\beta_2(2) = 2 < 3$ is proved below, and — on the evidence of the same measurement — at $(2, 3)$. The failure at $(2, 2)$ is witnessed by an explicit degree-two relation (Proposition 8.1), one degree below what counting alone can force.

What rests on computation. Every independence statement in this paper is a statement that one explicit matrix of integers is nonsingular, and each is proved by exhibiting a left inverse modulo a prime. The verifications are exhaustive over finite index sets, and their sizes are stated in each proof; the largest formal one checks 816^2 matrix entries and one 816×816 modular matrix product. Section 9 says what is machine-checked and what is not. The statements that lie outside the formal development — the counting upper bound, whose formalisation needs a dimension formula not available to us in the library, and the extensions of the two tables beyond the certified range — are labelled as such where they occur, and nothing formal depends on them.

Provenance. The abstract page of [1] lists only v1 and carries no journal reference (checked 3 September 2026); a bibliographic database lookup returns no citing works, and the single citation reported by a second service is by the same author and does not mention the conjecture, so no later treatment of Conjecture 1.1 or of β_2 appears to exist. A full-text search of a local mirror of the mathematics sections of the arXiv found no paper referring to [1], and none stating a theorem, a

conjecture or a name for the assertion "$\mathrm{Sym}^3 V \to S_6$ has maximal rank for a general m-dimensional space V of quadrics". The one published source of values is [2, Table 1], which lists the degrees of the minimal generators of the ideal of relations among n generic squares of linear forms in d variables for $d \le 6$; that paper is not cited by [1], and its §3 states, verbatim, "Not much is known about the ideals of such projections in general". Its Table 1 stops at $d = 6$ in both versions that exist: we read the entries quoted below from the e-print of 20 October 2025, and that table is character-for-character the one in the first e-print of 25 May 2025, each paper having exactly one table. The sequence $4, 7, 9, 13, 16, 20, 25, 30, 35, 41, 47$ of §5 is not in the OEIS. The residual risk for Theorem 1.2 is an unpublished computer algebra computation by the authors of [2] or of [1].

2. Preliminaries

Throughout, $\mathbb{K}$ is a field of characteristic zero, $S = \mathbb{K}[X_1, \dots, X_n]$, and for a list $q = (q_1, \dots, q_m)$ of forms of a common degree k we abbreviate $I_{\mathrm{rel}}(q)$ as in §1. We index the three-fold products of q by *multisets*: write $T_m := \{(a, b, c) : 1 \le a \le b \le c \le m\}$, so $|T_m| = \binom{m+2}{3}$.

Lemma 2.1. *For $q_1, \dots, q_m \in S_k$ the following are equivalent.*

(i) $I_{\mathrm{rel}}(q)_{\le 3} = \{0\}$*;*
(ii) $I_{\mathrm{rel}}(q)$ *contains no nonzero form of degree exactly* 3*;*
(iii) the $\binom{m+2}{3}$ *products* $q_a q_b q_c$*,* $(a, b, c) \in T_m$*, are linearly independent in* S_{3k}*.*

Proof. (ii)⇔(iii): the monomials $Y_a Y_b Y_c$ with $(a, b, c) \in T_m$ are a basis of $\mathbb{K}[Y]_3$, and φ_q maps that basis to the list of products; a nonzero element of $I_{\mathrm{rel}}(q)_3$ is exactly a nontrivial vanishing linear combination of them. (i)⇒(ii) is trivial. For (ii)⇒(i), note first that a nonzero constant is not a relation. If $0 \ne F \in I_{\mathrm{rel}}(q)_d$ with $d \in \{1, 2\}$ then $Y_1^{3-d} F$ is nonzero, because $\mathbb{K}[Y]$ is a domain, is homogeneous of degree 3, and satisfies $\varphi_q(Y_1^{3-d} F) = q_1^{3-d} \varphi_q(F) = 0$; so $I_{\mathrm{rel}}(q)_3 \ne \{0\}$. Finally $I_{\mathrm{rel}}(q)$ is homogeneous: if $F = \sum_d F_d$ with $\varphi_q(F) = 0$, then $\varphi_q(F_d) \in S_{kd}$ and distinct d give distinct degrees, so each $\varphi_q(F_d) = 0$. □

For $k = 2$ the ambient space in (iii) is S_6, of dimension $\binom{n+5}{6}$. We write

$$\mathrm{mmax}(n) \;:=\; \max\Big\{\, m \;:\; \tbinom{m+2}{3} \le \tbinom{n+5}{6} \,\Big\},$$

the largest number of quadratic forms whose three-fold products could conceivably be independent. The first values are

n	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\mathrm{mmax}(n)$	2	4	7	9	13	16	20	25	30	35	41	47	53	60	67

Definition 2.2. For $n \ge 2$ let G_n be the set of triples (i, j, k) of residues modulo n with $i \le j \le k$ and $i + j + k \equiv 0 \pmod n$, and let the *Taveira Blomenhofer family* be $\{(X_i + X_j + X_k)^2 : (i, j, k) \in G_n\}$. (We index variables by $\{0, \dots, n-1\}$; [1] uses $\{1, \dots, n\}$, which is the same set of multisets of residues.)

The cardinality $|G_n|$ is the number of multisets $\{x, y, z\}$ of residues modulo n summing to 0, namely $(n^2 + 3n + 2\gcd(3, n))/6$, which equals the $\lceil (n+2)(n+1)/6 \rceil$ of Conjecture 1.1 for every n; it is entry $A007997(n+5)$ of the OEIS [4], whose first comment describes exactly this count. At $n = 7$ the family has 12 members, indexed by

$$\begin{array}{llll} (0,0,0), & (0,1,6), & (0,2,5), & (0,3,4), \\ (1,1,5), & (1,2,4), & (1,3,3), & (2,2,3), \\ (2,6,6), & (3,5,6), & (4,4,6), & (4,5,5). \end{array}$$

3. The counting bound

The bound recorded in [1] counts relations of degree one: m quadratic forms in a space of dimension $\binom{n+1}{2}$ must be linearly dependent once $m > \binom{n+1}{2}$. Counting one degree up is much sharper.

Proposition 3.1. *For all $n \geq 1$ and all fields $\mathbb{K}$, $\beta_2(n) \leq \operatorname{mmax}(n)$. Consequently $\beta_2(n)$ is finite, and*

$$\operatorname{mmax}(n) = \bigl(1 + o(1)\bigr)\,\frac{n^2}{120^{1/3}}, \qquad 120^{1/3} = 4.93242\ldots$$

Proof. Let $q_1, \ldots, q_m \in S_2$ with $m > \operatorname{mmax}(n)$. The $\binom{m+2}{3}$ products $q_a q_b q_c$, $(a,b,c) \in T_m$, all lie in S_6, and $\binom{m+2}{3} > \binom{n+5}{6} = \dim_{\mathbb{K}} S_6$ by the definition of $\operatorname{mmax}(n)$; so they are linearly dependent, and by Lemma 2.1 the family has a nonzero relation of degree three. For the asymptotics, $\binom{m+2}{3} = \frac{m^3}{6}(1+O(m^{-1}))$ and $\binom{n+5}{6} = \frac{n^6}{720}(1+O(n^{-1}))$, so the defining inequality reads $m^3 \leq \frac{n^6}{120}(1+O(n^{-1}))$. □

Proposition 3.1 is elementary, and we make no claim of novelty for the argument itself; the technical overview of [3] performs the same count asymptotically, with m^3 in place of $\binom{m+2}{3}$ and $\binom{n+5}{6} \sim n^6/720$ written out, but does not turn it into a bound on β_2. We could not find the inequality $\beta_2(n) \leq \operatorname{mmax}(n)$ stated anywhere, and it is not the bound [1] records: the improvement factor tends to $120^{1/3}/2 = 2.4662\ldots$, and $\operatorname{mmax}(n)$ exceeds the size $\sim n^2/6$ of the conjectured family by a factor tending to $6/120^{1/3} = 1.2164\ldots$ Numerically:

n	3	4	5	6	7	8	9	10	11	12	13
$\binom{n+1}{2}$ (the bound of [1])	6	10	15	21	28	36	45	55	66	78	91
$\operatorname{mmax}(n)$ (Proposition 3.1)	4	7	9	13	16	20	25	30	35	41	47
$\lvert G_n\rvert$ (Conjecture 1.1)	4	5	7	10	12	15	19	22	26	31	35

Proposition 3.1 is proved on paper and is *not* part of the formal development: it needs $\dim_{\mathbb{K}} S_6 = \binom{n+5}{6}$ for a symbolic n, which we did not find in the library we used. What is machine-checked is the arithmetic on which it is applied — the two inequalities $\binom{\operatorname{mmax}(n)+2}{3} \leq \binom{n+5}{6} < \binom{\operatorname{mmax}(n)+3}{3}$ for $n = 2, \ldots, 16$ (Proposition 7.1(d)) — so that the numbers $\operatorname{mmax}(n)$ used below are certified even though the dimension count above them is not.

4. Certificates

All positive results below are instances of one lemma, whose hypotheses are finite arithmetic over $\mathbb{N}$.

Lemma 4.1. *Let $\mathbb{K}$ have characteristic zero, let $p > 1$, let $q_0, q_1, \cdots \in S$ be polynomials with nonnegative integer coefficients, let $x_0, \ldots, x_{r-1} \in \mathbb{N}^n$, and let $V(a,s) \in \mathbb{N}$ satisfy $q_a(x_s) = V(a,s)$. Let (a_t, b_t, c_t), $t = 0, \ldots, r-1$, be index triples, and suppose two matrices $E, B \in \mathbb{N}^{r\times r}$ satisfy*

$$E_{ts} \equiv V(a_t,s)\,V(b_t,s)\,V(c_t,s) \pmod p \quad \text{and} \quad \sum_{u<r} B_{iu}E_{uj} \equiv \delta_{ij} \pmod p$$

for all $t, s, i, j < r$. Then the r products $q_{a_t}q_{b_t}q_{c_t}$ are linearly independent over $\mathbb{K}$.

Proof. Let $M \in \mathbb{Z}^{r\times r}$ be the integer matrix $M_{ts} = V(a_t,s)V(b_t,s)V(c_t,s)$. The second hypothesis says that the reduction of M modulo p admits a left inverse, so $\det M$ is invertible in $\mathbb{Z}/p$ and in particular $\det M \neq 0$ in $\mathbb{Z}$. Since $\mathbb{K}$ has characteristic zero, $\mathbb{Z} \hookrightarrow \mathbb{K}$, so the image of M in $\mathbb{K}^{r\times r}$ is invertible. Now evaluation at x_s is a $\mathbb{K}$-linear map $S \to \mathbb{K}$, and it sends $q_{a_t}q_{b_t}q_{c_t}$ to M_{ts}; so a vanishing linear combination $\sum_t g_t\, q_{a_t}q_{b_t}q_{c_t} = 0$ with $g \in \mathbb{K}^r$ gives $\sum_t g_t M_{ts} = 0$ for every s, i.e. $gM = 0$, whence $g = 0$. □

Two design points make the lemma usable. First, the certificate is an *evaluation* matrix, not a coefficient matrix: the products are never expanded, and the object to be inverted is $r \times r$ rather than $r \times \binom{n+5}{6}$. This is also what makes the present verification of Conjecture 1.1 at $n = 7$ independent of the one reported in [1], which works with coefficients. Second, neither the points nor the left inverse are carried as data. The points are given by the closed formula

$$x_s(i) \;=\; \big(s^2 + s(i+1) + 1\big) \bmod \pi_i, \qquad (\pi_0, \pi_1, \pi_2, \dots) = (11, 13, 17, 19, 23, 29, 31, \dots),$$

and B is computed inside the checked computation by Gauss–Jordan elimination modulo $p = 65521$. The prime is deliberately below 2^{16}, so that the sums $\sum_u B_{iu}E_{uj}$ stay below $r\,p^2 < 2^{42}$ at every size $r \le 816$ used here, and the checking arithmetic never leaves machine words.

Remark 4.2. The choice of point set is a matter of search, not of soundness — a bad choice makes no certificate exist, and can never make a false one succeed — but it is what decides whether the method works at all. If each coordinate $x_s(i)$ is a polynomial of degree $\le D$ in s over the coefficient field, the points lie on a rational curve, a degree-6 form restricted to it is a polynomial of degree $\le 6D$ in s, and the evaluation matrix has rank at most $6D + 1$ however many points are used; if instead the formula is periodic in s with period B, the rank is at most B. We observed both ceilings before settling on the formula above: reduction of the *same* quadratic in s by *different* small primes in different coordinates is neither polynomial over the coefficient field nor short-period, and it produced a nonsingular matrix at every size and every prime we tried.

5. The value of $\beta_2(n)$

The certificates below use squares of linear forms with one-digit coefficients read off a single fixed stream of 112 decimal digits,

```
65191661411063  37884867822272  82974254195317  20382779214289
59762354393375  97885332784990  05060358352400  02457335668169
```

(read left to right, then top to bottom) by taking the first mn digits n at a time: the a-th linear form is $\ell_a = \sum_{i=1}^{n} d_{(a-1)n+i} X_i$ and the a-th quadric is ℓ_a^2. Thus at $n = 7$, $m = 16$ the sixteen forms are $6X_1 + 5X_2 + X_3 + 9X_4 + X_5 + 6X_6 + 6X_7$, $X_1 + 4X_2 + X_3 + X_4 + 6X_6 + 3X_7$, and so on. Nothing depends on the stream being this one; it was produced by a search over random digit vectors, stopped at the first success.

Theorem 5.1. *Let $\mathbb{K}$ be any field of characteristic zero.*

1. *The $\binom{9}{3} = 84$ three-fold products of the 7 squares of linear forms in 4 variables read off the stream above are linearly independent over $\mathbb{K}$. Hence $\beta_2(4) \ge 7$.*
2. *The $\binom{11}{3} = 165$ three-fold products of the 9 squares of linear forms in 5 variables read off the stream above are linearly independent over $\mathbb{K}$. Hence $\beta_2(5) \ge 9$.*
3. *The $\binom{15}{3} = 455$ three-fold products of the 13 squares of linear forms in 6 variables read off the stream above are linearly independent over $\mathbb{K}$. Hence $\beta_2(6) \ge 13$.*

Proof. Each case is Lemma 4.1 with $p = 65521$, $r = 84$, 165, 455, the points of §4, and B the Gauss–Jordan inverse of the value matrix modulo p. The finite checks are exhaustive: for each case, all r^2 entries of the reduced value matrix are recomputed from the linear forms and compared, and all r^2 entries of the product BE are computed modulo p and compared with the identity — $84^2 + 84^2$, $165^2 + 165^2$ and $455^2 + 455^2$ comparisons respectively. The passage from independence to $\beta_2(n) \ge m$ is Lemma 2.1. □

The three values $7, 9, 13$ are not new. They are what [2, Table 1] gives, once combined with Proposition 3.1: that table lists the degrees of the minimal generators of the ideal of relations among n generic squares of linear forms in d variables for $d \le 6$, and the last row for $d = 4$ with no generator in degree ≤ 3 is $n = 7$, the first with one being $n = 8$; likewise $9, 10$ for $d = 5$ and $13, 14$ for $d = 6$, and $4, 5$ for $d = 3$. So that table already supplies the lower bounds $\beta_2(d) \ge 4, 7, 9, 13$ for $d = 3, 4, 5, 6$, and since these equal $\mathrm{mmax}(d)$ they are the values. What Theorem 5.1 adds is a

certificate, valid over every field of characteristic zero rather than for a generic choice, and a control on the method before it is applied past the published range. The next case is past that range.

Theorem 5.2. *Let $\mathbb{K}$ be any field of characteristic zero. The $\binom{18}{3} = 816$ three-fold products of the 16 squares of linear forms in 7 variables read off the stream above are linearly independent over $\mathbb{K}$. Hence $\beta_2(7) \geq 16$.*

Proof. Lemma 4.1 with $r = 816$, $p = 65521$ and the points of §4. The two finite checks are exhaustive over the $816^2 = 665\,856$ index pairs each: that the stored 816×816 matrix agrees modulo p with the value matrix of the 816 products at the 816 points, and that its stored Gauss–Jordan left inverse multiplies it to the identity modulo p. Lemma 2.1 converts independence into $\beta_2(7) \geq 16$. □

Corollary 5.3. *$\beta_2(n) = \mathrm{mmax}(n)$ for $3 \leq n \leq 7$, with values $4, 7, 9, 13, 16$. In particular $\beta_2(7) = 16$, four more than the 12 quadrics that Conjecture 1.1 supplies at $n = 7$, and the family of Conjecture 1.1 is not extremal for any n with $4 \leq n \leq 7$.*

Proof. The upper bounds are Proposition 3.1 together with the certified arithmetic of Proposition 7.1(d), which gives $\mathrm{mmax}(n) = 4, 7, 9, 13, 16$ for $n = 3, \ldots, 7$. The lower bounds are Theorems 5.1 and 5.2 for $n = 4, 5, 6, 7$ and [2, Table 1] for $n = 3$. The sizes $|G_n| = 4, 5, 7, 10, 12$ are Proposition 7.1(a), and $|G_n| < \mathrm{mmax}(n)$ for $4 \leq n \leq 13$ is Proposition 7.1(e). □

It is worth saying why Theorem 5.2 is not a formality. The naive expectation is that a general family of $\mathrm{mmax}(n)$ quadrics has independent products, the counting bound being attained because a general linear map between spaces of these dimensions has maximal rank. One degree lower that expectation fails: for eight generic squares of linear forms in four variables the $\binom{9}{2} = 36$ two-fold products span a space of dimension 34, not 35, so there are *two* independent relations of degree two where counting predicts one. We verified this by an exact rank computation, for squares of linear forms and for general quadrics alike, and it matches the entry for $(d, n) = (4, 8)$ in [2, Table 1], which records two minimal generators of degree two. A defective case one degree below is exactly the reason to want a certificate rather than an appeal to genericity.

Computation 5.4 (outside the formal development). $\beta_2(n) = \mathrm{mmax}(n) = 20, 25, 30, 35$ for $n = 8, 9, 10, 11$. For each such n we drew $\mathrm{mmax}(n)$ quadrics over the field with $p = 10^9 + 7$ elements, once as general symmetric forms and once as squares of random linear forms, and computed the rank of the matrix of values of their $\binom{\mathrm{mmax}(n)+2}{3}$ three-fold products at $\binom{n+5}{6} + 64$ random points, enough points that the evaluation rank equals the coefficient rank. Both classes gave the full ranks 1540, 2925, 4960, 7770 at every n. With Proposition 3.1 this determines $\beta_2(n)$; a nonsingular matrix over $\mathbb{Z}/p$ lifts the conclusion to characteristic zero exactly as in Lemma 4.1, but the computation itself was carried out outside the proof assistant and is recorded as a measurement, not as a theorem of this paper. The whole sweep cost about ten minutes of processor time. The corresponding sizes of the family of Conjecture 1.1 are $15, 19, 22, 26$.

Together with Corollary 5.3, Computation 5.4 says that the counting bound is attained at every $n \leq 11$ where the question has been decided, already by squares of linear forms; so on present evidence $\beta_2(n)$ grows like $n^2/4.932$, not like the $n^2/6$ of the conjectured family nor like the $n^2/2$ of the bound recorded in [1]. Whether $\beta_2(n) = \mathrm{mmax}(n)$ for all n we do not know; the $(4, 8)$ defect above shows that a proof cannot be a pure dimension count.

6. The family of Conjecture 1.1

Theorem 6.1. *Let $\mathbb{K}$ be any field of characteristic zero. The $\binom{14}{3} = 364$ three-fold products $q_\alpha q_\beta q_\gamma$, $\alpha \leq \beta \leq \gamma$, of the 12 quadrics $q_{ijk} = (X_i + X_j + X_k)^2$ indexed by G_7 are linearly independent over $\mathbb{K}$. Equivalently, I_{rel} of that family vanishes in degrees ≤ 3: Conjecture 1.1 holds at $n = 7$.*

Proof. Lemma 4.1 with $r = 364$, $p = 65521$, the twelve generators listed after Definition 2.2, and the points of §4; the finite checks are exhaustive over the $364^2 = 132\,496$ index pairs each, one comparing

the stored matrix with the value matrix modulo p and one verifying that the Gauss–Jordan left inverse multiplies it to the identity modulo p. The equivalence with the vanishing of the relation ideal in degrees ≤ 3 is Lemma 2.1, and the generator count $|G_7| = 12$ is Proposition 7.1(a). □

The statement of Theorem 6.1 is within the range $n \in \{7, \dots, 12\}$ that [1] reports as verified, so the mathematics is that paper's; we claim only the independent method and the formal certificate. The range itself we reproduced before going past it.

Computation 6.2 (outside the formal development). Conjecture 1.1 holds for every $n \le 16$. Writing $m = |G_n|$ and $r = \binom{m+2}{3}$, the matrix of values of the r products at $r + 64$ random points of $(\mathbb{Z}/p)^n$ has rank r in every case. The table records $7 \le n \le 16$; the cases $n \le 6$, which [1] does not mention, were checked in the same way and also hold.

n	7	8	9	10	11	12	13	14	15	16
m	12	15	19	22	26	31	35	40	46	51
$r = \binom{m+2}{3}$	364	680	1330	2024	3276	5456	7770	11480	17296	23426
$\dim S_6 = \binom{n+5}{6}$	924	1716	3003	5005	8008	12376	18564	27132	38760	54264
processor time	0.01 s	0.07 s	0.6 s	2 s	11 s	49 s	154 s	627 s	1770 s	3607 s

The columns $n \le 12$ reproduce, by the evaluation method of §4 rather than by coefficients, exactly the range [1] reports as verified. The columns $n = 13, \dots, 16$ go past it; $n = 13$ is the first case left open there. The case $n = 13$ was run twice, at $p = 10^9 + 7$ and at $p = 2^{31} - 1$, with independent random point sets, since it is the first new one; a rank deficiency would in any case be inconclusive and would be retried with fresh points, and none occurred. The four new cases cost 1.7 hours of processor time in total and peaked at 2.06 gigabytes. As in Computation 5.4, full rank over $\mathbb{Z}/p$ implies independence over every field of characteristic zero, but these computations were not carried out in the proof assistant and are recorded as measurements.

7. Controls

A development in which every theorem asserts the independence of an explicit list can be satisfied by the wrong list. The following are checked to guard against that; all are exhaustive finite verifications except (f) and (g), which are proved symbolically.

Proposition 7.1. *(a)* $|G_n| = 2, 4, 5, 7, 10, 12, 15, 19, 22, 26, 31, 35$ *for* $n = 2, \dots, 13$*, matching the count* $\lceil (n+2)(n+1)/6 \rceil$ *stated in* [1].

(b) $|G_7| \ne 11$ *and* $|G_7| \ne 13$*: neither neighbour of the value used in Theorem 6.1 is the generator count.*

(c) $|T_m| = 84, 165, 364, 455, 816$ *for* $m = 7, 9, 12, 13, 16$*, the sizes used by the certificates.*

(d) For $n = 2, \dots, 16$*:* $\binom{\mathrm{mmax}(n)+2}{3} \le \binom{n+5}{6} < \binom{\mathrm{mmax}(n)+3}{3}$*, with* $\mathrm{mmax}(n)$ *the values tabulated in §2. So each certificate above sits exactly at the largest size the counting bound permits.*

(e) $|G_n| < \mathrm{mmax}(n)$ *for* $n = 4, \dots, 13$*: the family of Conjecture 1.1 is strictly below the counting bound from* $n = 4$ *on.*

(f) Over every commutative ring, $\big((X_1 + X_2)^2 - X_1^2 - X_2^2\big)^2 = 4X_1^2X_2^2$*; that is,* $Y_3, Y_1, Y_2 \mapsto (X_1 + X_2)^2, X_1^2, X_2^2$ *kills the nonzero form* $(Y_3 - Y_1 - Y_2)^2 - 4Y_1Y_2$ *of degree two.*

(g) Two index triples differing by a permutation give the same product, so the two-element list they index is never linearly independent: every positive result above would be false with all ordered triples in place of the multisets T_m*.*

Item (f) is also the sharpest available witness that the counting bound of Proposition 3.1 is not vacuous: $\mathrm{mmax}(2) = 2$, and one quadric past that bound the relation is not merely forced in degree three, it is exhibited in degree two. It is used again in §8.

8. A remark of the source

Remark 4.3 of [1], stated as motivation for the inequality $\beta_k(n) \geq n+1$, reads: for $m = n+1$, $k \geq 2$ and general $q_1, \ldots, q_m \in \mathbb{K}[X]_k$, the ideal of relations is principal, $I_{\mathrm{rel}}(q_1, \ldots, q_m) = (f)$, with $\deg f = k^n$; "by Bézout's theorem and genericity" the relevant system has k^n complex solutions; and hence, for all $n \geq 2$ and $k \geq 2$, $\beta_k(n) \geq n+1$. The exponent is one too large, and the conclusion consequently fails at two pairs: Proposition 8.1 settles $(n,k) = (2,2)$ outright, and Computation 8.2 is the evidence for the degree and for $(2,3)$. We state this plainly because the remark is an aside — no theorem of [1] depends on it — and because the paper is a preprint with no erratum: the point is a correction to the record, not a criticism of the results there.

Proposition 8.1. *$\beta_2(2) = 2$. In particular $\beta_k(n) \geq n+1$ fails at $(n,k) = (2,2)$. Two independent reasons:* $\mathrm{mmax}(2) = 2$ *by Proposition 7.1(d), so Proposition 3.1 already forbids three quadratic forms in two variables from avoiding a relation of degree three; and, one degree lower than counting can see, the three squares X_1^2, X_2^2, $(X_1+X_2)^2$ satisfy the explicit nonzero relation $(Y_3-Y_1-Y_2)^2-4Y_1Y_2$ of degree two of Proposition 7.1(f).*

Proof. $\beta_2(2) \leq \mathrm{mmax}(2) = 2$ is Proposition 3.1 with the certified arithmetic $\binom{4}{3} \leq \binom{7}{6} < \binom{5}{3}$, i.e. $4 \leq 7 < 10$. For $\beta_2(2) \geq 2$, the four products $X_1^6, X_1^4X_2^2, X_1^2X_2^4, X_2^6$ of $q_1 = X_1^2$, $q_2 = X_2^2$ are distinct monomials, hence independent. For the second reason, the three quadrics of Proposition 7.1(f) are a basis of the three-dimensional space of binary quadratic forms, so any three linearly independent binary quadratics are their image under an invertible linear substitution of the Y's, which carries the exhibited relation to a nonzero relation of degree two; and three linearly dependent ones have a relation of degree one. □

Computation 8.2 (outside the formal development). For $m = n+1$ general k-forms in n variables, the least degree at which the products become dependent — equivalently, the degree of the generator of I_{rel}, which we found to be principal in the sense that the space of relations in that least degree is one-dimensional — is k^{n-1}, not k^n. Exact ranks of coefficient matrices modulo $2^{61}-1$ for random forms give

(n,k)	$(2,2)$	$(2,3)$	$(2,4)$	$(2,5)$	$(3,2)$	$(3,3)$	$(4,2)$
measured $\deg f$	2	3	4	5	4	9	8
k^{n-1}	2	3	4	5	4	9	8
k^n (as asserted in [1])	4	9	16	25	8	27	16

The same values arise for general squares of linear forms as for general quadrics, and for the family of Conjecture 1.1 at $n = 3$ and $n = 4$, the two values of n at which $|G_n| = n+1$; so that family has minimal relation degree 4 at $n = 3$ and 8 at $n = 4$.

The geometric reason is a degree count. For general $q_1, \ldots, q_{n+1} \in \mathbb{K}[X_1, \ldots, X_n]_k$ the forms have no common zero in $\mathbb{P}^{n-1}$, so they define a morphism $\bar{q}\colon \mathbb{P}^{n-1} \to \mathbb{P}^n$ whose image Y is a hypersurface, and $I_{\mathrm{rel}}(q)$ is the homogeneous ideal of Y, generated by one form f of degree $\deg Y$. Pulling back $n-1$ general hyperplanes — which is what cuts out a general line $L \subset \mathbb{P}^n$ — gives $n-1$ forms of degree k on $\mathbb{P}^{n-1}$, so by Bézout $\deg(\bar{q}) \cdot \deg Y = k^{n-1}$. The remark of [1] instead pulls back n hyperplanes, one more than a line in $\mathbb{P}^n$ requires; the resulting n forms of degree k in n variables have no common zero away from the origin, so the Bézout number k^n that this produces is not counting the points of $Y \cap L$.

To turn $\deg(\bar{q}) \cdot \deg Y = k^{n-1}$ into $\deg f = k^{n-1}$ one needs $\deg(\bar{q}) = 1$, that is, $\bar{q}$ birational onto its image. We have not proved this and do not claim it: $\bar{q}$ is the k-uple Veronese embedding of $\mathbb{P}^{n-1}$ followed by a linear projection whose centre is general, and the target $\mathbb{P}^n$ has dimension one more than the source, which is the situation in which a general projection is expected to be generically injective; but we could not locate a reference stating it in the form we need, and we did not supply a proof. We therefore record $\deg(\bar{q}) = 1$ as a hypothesis of this explanation. It is only an explanation: the assertion we test is $\deg f = k^{n-1}$ itself, and Computation 8.2 finds exactly that

at seven pairs (n,k), in each case with a one-dimensional space of relations in that degree. The correction to the record does not depend on the hypothesis either — at $(n,k)=(2,2)$ the relation of degree $2<4=k^n$ is exhibited outright in Proposition 8.1.

Two consequences. With the corrected degree, the conclusion of the remark is restored whenever $k^{n-1}>3$, that is for all $n\geq 3$ and for $n=2$ with $k\geq 4$. And at the two remaining pairs it fails: at $(2,2)$ by Proposition 8.1, which rests on no computation of degrees at all, and at $(2,3)$, where $\beta_3(2)=2$ as well. The pair $(2,3)$ is instructive because counting cannot see it: $\binom{5}{3}=10$ equals $\dim \mathbb{K}[X_1,X_2]_9=10$ exactly, so no relation is forced, yet three general binary cubics do satisfy one — their image in $\mathbb{P}^2$ is a plane cubic, cut out by a single form of degree three, in agreement with Computation 8.2 at $(n,k)=(2,3)$. That $\beta_3(2)\geq 2$ holds is immediate from the four distinct monomials $X_1^9, X_1^6X_2^3, X_1^3X_2^6, X_2^9$; the matching upper bound is the measurement.

9. Verification

Lemma 4.1, Theorems 5.1, 5.2 and 6.1 and Proposition 7.1 are formalised and machine-checked in Lean 4 [5] against Mathlib [6], in five modules: the objects, the point formula, the modular Gauss–Jordan routine and Lemma 4.1 (215 lines); the certificate of Theorem 6.1 (83 lines); those of Theorem 5.1 together with the counting arithmetic for $n=3,\dots,8$ (201 lines); that of Theorem 5.2 (69 lines); and the controls (122 lines). There is no `sorry` anywhere and we declare no axiom of our own; Lemma 4.1 and the two symbolic controls Proposition 7.1(f),(g) use only the three standard logical axioms of the library, and the counting arithmetic for $n\leq 8$ is checked by kernel reduction alone. Each of the four independence theorems rests on exactly two exhaustive evaluations, carried out by Lean's compiled evaluator (`native_decide`), namely the two hypotheses of Lemma 4.1: that the stored $r\times r$ matrix agrees modulo $p=65521$ with the value matrix of the r products at the r points, and that the Gauss–Jordan left inverse — itself computed inside the evaluation, not stored — multiplies it to the identity modulo p; each such evaluation contributes one axiom of its own, and nothing else in the development depends on the evaluator except the finite tables of Proposition 7.1(a)–(e), one evaluation each. Checking the files costs, on one machine, 10, 147, 332, 1745 and 7 seconds of processor time respectively — wall-clock times were several times larger, the machine being shared — and each stays within a gigabyte of the memory that importing the library already costs; the computations of §5 and §6 that lie outside the proof assistant, and the searches that produced the digit stream and the point formula, cost about 2.2 hours of processor time in total and peaked at 2.06 gigabytes. Proposition 3.1, Lemma 2.1, Computations 5.4, 6.2 and 8.2, the $(4,8)$ defect quoted in §5, the $\beta_3(2)$ discussion and the degree count of §8 are outside the formal development and are labelled where they occur. The repository is private: repository reference to be added at submission.

10. The frontier

Three natural next steps have been priced rather than taken. For Conjecture 1.1, the case $n=17$ has $r=32\,509$ and is estimated at 2.3 hours of processor time and 4.2 gigabytes, which is feasible; $n=18$ has $r=45\,760$ and is estimated at 6.4 hours and 8.4 gigabytes, which we did not attempt. For β_2, the first case of Computation 5.4 not yet certified is $n=8$, where $r=1540$ and the elimination inside the checked computation is about seven times the $n=7$ one; that is past what the interpreted evaluator will do in reasonable time, and the route is to compile the checked module into a shared library, which would also bring $n=9,10$ within reach. Formalising Proposition 3.1 needs $\dim S_6=\binom{n+5}{6}$ for symbolic n; the route through the library's homogeneity predicate and the bijection between monomials of degree d and multisets of size d is clear but was not carried out. Beyond these, the question we cannot price is the one Corollary 5.3 and Computation 5.4 raise: whether $\beta_2(n)=\mathrm{mmax}(n)$ for all n. A degeneration argument is the obvious attack and carries an obvious obstruction — the initial form of $(X_i+X_j+X_k)^2$ under any weight order is a square of a single variable, and the map from index triples to that variable is far from injective, so no

argument by monomial triangularity in these coordinates can succeed. The minimal relation degree of the family of Conjecture 1.1 is another unexplored invariant: Computation 8.2 gives it at $n = 3, 4$, where the family happens to have $n + 1$ members, and from $n = 5$ on the relation ideal is no longer principal and nothing is known.

References

[1] A. Taveira Blomenhofer, *Unique powers-of-forms decompositions from simple Gram spectrahedra*, arXiv:2305.06860. Subject classification as given there: primary 14Q30, 15A69; secondary 62H12, 68Q25. All quotations above are from v1, dated 11 May 2023, the only version: the arXiv abstract page listed v1 alone, with no journal reference, when checked on 3 September 2026. In that version the conjecture is Conjecture 4.2 and the remark discussed in §8 is Remark 4.3, both on page 13, in the unnumbered subsubsection "First condition: Algebraic relations of general k-forms" of §4.1, "Real Geometry Viewpoint"; the definition of $\beta_k(n)$ is in the same subsubsection. We give these numbers as printed by the v1 source, and cite them as such, since a later version could renumber.

[2] H. Friedman, B. Sturmfels and M. Wiesmann, *Squared Linear Models*, SIAM J. Appl. Algebra Geom. **10** (2026), no. 2, 153–173; doi:10.1137/25M1763998; preprint arXiv:2505.19351. We read Table 1 — the degrees of the minimal generators of the ideal of relations among n generic squares of linear forms in d variables, for $d \leq 6$ — from the e-print of 20 October 2025 (v2), the latest version, on 3 September 2026; it is identical to the table in v1 of 25 May 2025, and each of those versions contains exactly one table. The journal version was not available to us, so the entries quoted here are cited from the e-print.

[3] M. Bafna, J.-T. Hsieh, P. K. Kothari and J. Xu, *Polynomial-Time Power-Sum Decomposition of Polynomials*, in: 2022 IEEE 63rd Annual Symposium on Foundations of Computer Science (FOCS), Denver, CO, USA, 31 October–3 November 2022, IEEE, 2022, pp. 956–967; doi:10.1109/FOCS54457.2022.00094; preprint arXiv:2208.00122. Section 6.4, "Singular value lower bounds for desymmetrization", of the e-print (v1, 30 July 2022, the only version; read 3 September 2026) is the section [1] cites for $\beta_2(n) = \Theta(n^2)$; the section numbering is the e-print's, which need not agree with the proceedings version. Its bounds are of the form $m \leq (\ell/\mathrm{polylog}\,\ell)^c$, with no explicit constant, and we did not find an upper bound on β_2 there.

[4] OEIS Foundation Inc., *Sequence A007997*, The On-Line Encyclopedia of Integer Sequences, https://oeis.org/A007997. Its first comment gives the number of solutions of $x + y + z \equiv 0$ with $0 \leq x \leq y \leq z < m$, which is $|G_n|$ for $m = n$; in the indexing of the entry, $|G_n| = A007997(n + 5)$.

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

[6] The mathlib Community, *The Lean mathematical library*, in: Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP 2020), ACM, 2020, pp. 367–381; doi:10.1145/3372885.3373824.