EXACT VALUES OF THE DE KLERK–LAURENT HYPERCUBE CONSTANTS: $C_4 = 1/24$, $C_6 = 1/48$, $C_{4,6} = 1/224$, AND VERTEX-DUAL LOWER BOUNDS

KOREA SUPERINTELLIGENCE LABS

ABSTRACT. For the hypercube $[0,1]^n$ with generators $g_i = x_i - x_i^2$, let $C_{n,2d}$ be the smallest constant such that $x_1 \cdots x_n + C_{n,2d}$ lies in the degree-$2d$ truncated quadratic module $M_{n,2d}(\mathbf{g})$, and let $C_n = C_{n,n}$. De Klerk and Laurent conjectured $C_n = 1/(n(n+2))$ for even n on the strength of a computer verification for $n = 2, 4, 6$ that they do not detail; Polak (arXiv:2605.31169) recently disproved the value at $n = 8$ and tabulated numerical values of $C_{n,2d}$, marking $1/224$ at $(n, 2d) = (4, 6)$ and $1/360$ at $(6, 8)$ as "suggested value from numerics". We prove $C_4 = 1/24$, $C_6 = 1/48$ and $C_{4,6} = 1/224$ exactly, and $C_{6,8} \geq 1/360$, $C_{6,10} \geq 1/3968$. The lower bounds are signed weightings of the 2^n cube vertices: since every generator vanishes at every vertex, such a weighting is a dual certificate for the truncated quadratic module as soon as its $0/1$ moment matrix of order d is positive semidefinite; the resulting relaxation is the Boolean-quotient relaxation that Polak discusses, and its exact rational optimum agrees with the numerical value of $C_{n,2d}$ at every cell with $2d \leq n+2$ treated here and is strictly smaller at $(6, 10)$. The upper bounds at $(4, 6)$ and $(6, 6)$ are exact rational Gram certificates of orders 35 and 84, found on the optimal face by complementary slackness against the exact dual and checked as integer polynomial identities by a certificate checker whose soundness theorem yields membership in the truncated module with bounded-degree multipliers. Four constants are thus known exactly (C_2, C_4, $C_{4,6}$, C_6); the bounds at $(6, 8)$ and $(6, 10)$ remain one-sided. Combined with a lemma of Polak, the exact values show that his Boolean-quotient constant $C^{\mathrm{bool}}_{n,n}$ equals C_n for $n = 2, 4, 6$. Every theorem is verified in Lean 4 with Mathlib.

1. INTRODUCTION

1.1. **The objects.** Let $H_n = [0,1]^n$ be the unit hypercube, described by the n inequalities $g_i = x_i - x_i^2 \geq 0$, and write $\mathbf{g} = (g_1, \ldots, g_n)$. For even $r = 2d$, the degree-r truncated quadratic module generated by $\mathbf{g}$ is, in the words of [2, §1], "the set of all polynomials of the form $p = \sigma_0 + \sum_{i=1}^n \sigma_i(x_i - x_i^2)$, where $\sigma_0, \sigma_1, \ldots, \sigma_n$ are sums of squares of polynomials, $\deg \sigma_0 \leq r$, and $\deg \sigma_i \leq r - 2$"; we denote it $M_{n,r}(\mathbf{g})$. Following [2, §4], $C_{n,2d}$ is the minimum constant such that $x_1 \cdots x_n + C_{n,2d} \in M_{n,2d}(\mathbf{g})$, and $C_n := C_{n,n}$. Equivalently, $-C_{n,2d}$ is the value of the degree-$2d$ Lasserre–Putinar relaxation [6] of $\min_{H_n} x_1 \cdots x_n$, whose true minimum is 0; so $C_{n,2d}$ is exactly the error of that relaxation on the monomial $x_1 \cdots x_n$.

1.2. **The source and its open questions.** The constant was introduced by De Klerk and Laurent in the concluding section of [1]. (We quote the author-accepted manuscript distributed by the authors, dated August 2010, whose equation numbers (4.3), (4.4) we use; the Optimization Online preprint of April 2010 has the same text with the numbers (38), (39). The published version was not accessed.) There they

describe the hypercube by $g_i = x_i - x_i^2$, write $M_r(\mathbf{g})$ for the truncated quadratic module with $\deg \sigma_0,\ \deg(\sigma_j g_j) \le r$, observe that the monomial $x_1 \cdots x_n$ "belongs to $M(\mathbf{g})$ after adding a suitable constant", namely that for n even $x_1 \cdots x_n + C_n \in M_n(\mathbf{g})$ "for some constant $C_n \le 1$" (their (4.3), with two proofs), and use this membership to convert Bernstein-type certificates on the hypercube into certificates in the quadratic module (their (4.4)). They then write: "We conjecture that for n even the smallest constant C_n for which (4.3) holds is $C_n = 1/n(n+2)$. We verified that this is true for $n = 2, 4, 6$ (using computer for $n = 4, 6$). For $n = 2$ the identity

$$x_1x_2 + \tfrac{1}{8} = \tfrac{1}{2}\big(x_1 + x_2 - \tfrac{1}{2}\big)^2 + \tfrac{1}{2}(x_1 - x_1^2) + \tfrac{1}{2}(x_2 - x_2^2) \tag{1}$$

shows $C_2 \le 1/8$." No detail of the computer verification is given. Polak [2, §1] summarizes this as: they "showed that such a constant $C_n \le 1$ exists, and conjectured that the smallest one is $C_n = 1/(n(n+2))$, suggested by their numerical verification for the cases $n = 2, 4, 6$ and a symbolic expression for the case $n = 2$", and he prints (1) multiplied by 8, as $8x_1x_2 + 1 = (1 - 2x_1 - 2x_2)^2 + 4g_1 + 4g_2$.

Polak [2] disproves the conjectured value two steps further on: his Theorem 1.1 exhibits an exact rational certificate for $C_8 \le 11/1000 < 1/80$. (All statement, table and section numbers of [2] quoted in this paper are those of arXiv:2605.31169v1, the only version at the time of writing, as read from the arXiv PDF.) He also prints, in his Table 1, numerical values of $C_{n,2d}$ obtained with SDPA-GMP for sixteen pairs $(n, 2d)$, and next to them a column headed "suggested value from numerics" which reads 1/8, 1/24, 1/48, 1/224, 1/360 in the rows $(2,2)$, $(4,4)$, $(6,6)$, $(4,6)$, $(6,8)$ and is blank in the other eleven rows. The sentence following the table is explicit about the status of these numbers: "The values in Table 1 are numerical SDP optima and are not used as proof of the main theorem." Thus, to our knowledge, no exact value of $C_{n,2d}$ had been proved for any $(n, 2d)$ before the present paper: the upper bounds $C_4 \le 1/24$ and $C_8 \le 11/1000$ are Polak's certificates, but the optimality of $1/24$ at $n = 4$ and of $1/48$ at $n = 6$ rested on De Klerk and Laurent's undocumented computer verification (numerical, according to Polak), and $1/224$, $1/360$ are values suggested by nine printed decimals. Polak's counterexample at $n = 8$ is precisely what makes these cases interesting, since the pattern $1/(n(n+2))$ is not safe to extrapolate. The quantitative literature on Putinar-type certificates over the hypercube—Baldi and Slot [3], who record the De Klerk–Laurent conjecture as open, and Gribling, de Klerk and Vera [4, 5]—concerns degree bounds and convergence rates, and states no value of, and no lower bound for, any $C_{n,2d}$.

Polak's final section [2, §6] adds a structural question. Let $I_n = \langle x_1^2 - x_1, \dots, x_n^2 - x_n\rangle$ and let $C^{\mathrm{bool}}_{n,2d}$ be the smallest C such that $x_1 \cdots x_n + C \equiv \sum_j q_j^2 \pmod{I_n}$ with $\deg q_j \le d$. His Lemma 6.1 shows $C^{\mathrm{bool}}_{n,2d} = C^{\mathrm{pre}}_{n,2d} \le C_{n,2d}$, where $C^{\mathrm{pre}}_{n,2d}$ is the analogous constant for the truncated preordering, and he states that, after averaging over S_n, the dual of the Boolean relaxation takes the form

$$C^{\mathrm{bool}}_{n,2d} = \max_{y_0,\dots,y_n \in \mathbb{R}} \Big\{ -y_n :\ y_0 = 1,\ \big(y_{|A \cup B|}\big)_{A,B \subseteq [n],\ |A|,|B| \le d} \succeq 0 \Big\}. \tag{2}$$

Numerically he finds $C^{\mathrm{bool}}_{n,n} = C_n$ for $n = 2, 4, \dots, 12$ and asks (Problem 1) whether $C^{\mathrm{bool}}_{n,n} = C_n$ for every even n.

1.3. **What is settled here.** Our results are collected in Table 1. Thus the De Klerk–Laurent value $1/(n(n+2))$ is optimal at $n = 4$ and at $n = 6$, both of Polak's

n	$2d$	numerical	suggested	lower bound	upper bound	exact value
2	2	0.125000000	1/8	1/8 (4.1)	1/8 (4.1)	$C_2 = 1/8$
4	4	0.041666667	1/24	1/24 (4.2)	1/24 (4.2)	$C_4 = 1/24$
4	6	0.004464286	1/224	1/224 (4.4)	1/224 (4.3)	$C_{4,6} = 1/224$
6	6	0.020833333	1/48	1/48 (4.6)	1/48 (4.5)	$C_6 = 1/48$
6	8	0.002777778	1/360	1/360 (5.1)	—	open
6	10	0.000310382	—	1/3968 (5.2)	—	open (bound not tight)

TABLE 1. The cells of Polak's Table 1 treated in this paper. The numerical values and the "suggested value from numerics" column are copied from [2, Table 1]; the last three columns are what is proved here, with the number of the proposition or theorem in parentheses. A lower bound is a vertex-dual certificate (Section 3), an upper bound a membership certificate; a cell with both is an exact value.

suggested off-diagonal values are correct lower bounds, and one of them (1/224) is the exact value. Precisely four constants are two-sided, i.e. known exactly: C_2, C_4, $C_{4,6}$ and C_6. The two remaining bounds are one-sided: at $(6, 8)$ we prove the lower bound $1/360$ and have no matching membership certificate, and at $(6, 10)$ the lower bound $1/3968$ is the exact optimum of the lower-bound relaxation but lies strictly below the numerical value 0.000310382 of $C_{6,10}$, so the last line records where the method stops.

The lower bounds all come from one device (Theorem 3.1): a signed weighting w of the 2^n vertices of the cube defines the functional $L_w(p) = \sum_{A\subseteq[n]} w_A\, p(1_A)$, and because every generator g_i vanishes at every 0/1 point, L_w annihilates every multiplier term $\sigma_i g_i$. So no localizing condition survives, and L_w is a dual certificate for $M_{n,2d}(\mathbf{g})$ as soon as $L_w(\sigma_0) \geq 0$ for every sum of squares σ_0 of degree $\leq 2d$, which is the single condition that the 0/1 moment matrix $\big(f_w(S \cup T)\big)_{|S|,|T|\leq d}$, $f_w(S) = \sum_{A\supseteq S} w_A$, be positive semidefinite. The relaxation obtained by optimizing over w is, after symmetrization, exactly the right-hand side of (2): we do not claim the relaxation as new, and Polak's Lemma 6.1 gives the same inequality $C^{\mathrm{bool}}_{n,2d} \leq C_{n,2d}$ from the primal side. What is new is that at each of the five cells with $2d \leq n+2$ in Table 1 the optimum of this relaxation is a small rational (proved at the four cells matched by a Gram certificate, numerical at $(6, 8)$), attained by an explicit rational moment matrix on the boundary of the cone, and that at four of the cells it is matched by an exact rational Gram certificate. The two large certificates, at $(4, 6)$ and $(6, 6)$, have Gram matrices of sizes 35×35 (rank 21) and 84×84 (rank 57).

A consequence of the exact values and Polak's Lemma 6.1 is that $C^{\mathrm{bool}}_{n,n} = C_n$ for $n = 2, 4, 6$ and $C^{\mathrm{bool}}_{4,6} = C_{4,6}$ (Remark 5.4); this answers Problem 1 of [2] affirmatively in the first three cases, where previously only numerical agreement was known.

Every theorem below has been checked by the Lean 4 proof assistant against the Mathlib library; Section 6 says what was checked, by which means, and under which axioms. Three of the certificates are large enough that their arithmetic is delegated to compiled code; everything else, including all of $C_4 = 1/24$ and $C_{4,6} = 1/224$, is checked by the kernel itself.

1.4. **What remains open.** The upper bound $C_{6,8} \le 1/360$; the exact value of $C_{6,10}$; the value of C_8 (the vertex relaxation reproduces Polak's numerical 0.010717341, but its optimum does not look like a small rational); and the cells $(2, 2d)$, $2d \ge 4$, where the vertex relaxation is useless (Remark 3.3).

1.5. **Changes from version 1.** No statement of the first version is changed or withdrawn. What is added: the membership halves of the two exact values at $(4, 6)$ and $(6, 6)$, which the first version treated inside the proofs of the exact-value theorems, are stated as theorems of their own (Theorems 4.3 and 4.5) together with their formal statements, so that each of the four exact values is now visibly the pair of a lower-bound theorem and an upper-bound theorem (the exact-value theorems of version 1, there numbered 4.3 and 4.4, are Theorems 4.4 and 4.6 here); Section 4.3 describes the data of the certificates and the soundness theorem of the checker that verifies them; the controls of Section 6 are stated as Proposition 6.1; Table 1 separates lower and upper bounds; and the axiom list of Appendix A was re-read for this version.

2. Preliminaries

Throughout, $n \ge 1$, $[n] = \{1, \dots, n\}$, and $\mathbb{R}[x] = \mathbb{R}[x_1, \dots, x_n]$. For a subset $A \subseteq [n]$ let $1_A \in \{0,1\}^n$ be its indicator vector, so $p(1_A)$ is the value of p at the vertex 1_A of the cube.

2.1. **Sums of squares and the truncated quadratic module.** For $k \in \mathbb{N}$ let Σ_k denote the set of polynomials of the form $\sum_{j=1}^{m} q_j^2$ with every $q_j \in \mathbb{R}[x]$ of total degree at most k (the empty sum 0 included). We use the module in the following "half-degree" form, which is the form the Lean development defines and the form of Polak's Gram-matrix reformulation [2, Corollary 2.2 and Proposition 3.3]: for $d \ge 1$,

$$\mathcal{M}_{n,d} := \Big\{ \sigma_0 + \sum_{i=1}^{n} \sigma_i \, (x_i - x_i^2) : \ \sigma_0 \in \Sigma_d, \ \sigma_1, \dots, \sigma_n \in \Sigma_{d-1} \Big\}. \tag{3}$$

$\mathcal{M}_{n,d}$ coincides with $M_{n,2d}(\mathbf{g})$ as defined in the introduction: a sum of squares of total degree at most $2d$ has every summand of degree at most d, because the leading forms of the squares cannot cancel. This elementary step is standard and is *not* part of the formal development; all theorems below are stated for $\mathcal{M}_{n,d}$ as defined in (3). (Polak's Corollary 2.2 and Proposition 3.3 likewise pass from $M_{n,2d}(\mathbf{g})$ to Gram matrices over the monomials of degree $\le d$ and $\le d-1$ without comment.) Set

$$\mathcal{F}_{n,d} := \{ c \in \mathbb{R} : x_1 x_2 \cdots x_n + c \in \mathcal{M}_{n,d} \}. \tag{4}$$

Since nonnegative constants are sums of squares, $\mathcal{F}_{n,d}$ is an up-set of $\mathbb{R}$. A statement "v is the least element of $\mathcal{F}_{n,d}$" therefore asserts two things: that $x_1 \cdots x_n + v \in \mathcal{M}_{n,d}$, and that $x_1 \cdots x_n + c \notin \mathcal{M}_{n,d}$ for every $c < v$. When it holds we write $C_{n,2d} = v$; this is Polak's $C_{n,2d}$, with the existence of the minimum included in the claim. A lower bound "$c \ge v$ for every $c \in \mathcal{F}_{n,d}$" is written $C_{n,2d} \ge v$, and a membership "$v \in \mathcal{F}_{n,d}$" (an upper bound) is written $C_{n,2d} \le v$; the two together are the statement $C_{n,2d} = v$.

2.2. **The vertex functional and the $0/1$ moment matrix.** For $w : 2^{[n]} \to \mathbb{R}$ define the linear functional and the upper-set transform

$$L_w(p) := \sum_{A \subseteq [n]} w_A \, p(1_A), \qquad f_w(S) := \sum_{A \supseteq S} w_A \quad (S \subseteq [n]). \tag{5}$$

Since $x^\alpha(1_A) = 1$ if $\operatorname{supp}\alpha \subseteq A$ and 0 otherwise, $L_w(x^\alpha) = f_w(\operatorname{supp}\alpha)$; in particular $f_w(\emptyset) = L_w(1)$ and $f_w([n]) = L_w(x_1 \cdots x_n)$. For $d \in \mathbb{N}$ let $\binom{[n]}{\le d}$ be the set of subsets of $[n]$ of size at most d, and let

$$M_d(f_w) := \big(f_w(S \cup T)\big)_{S,\,T \in \binom{[n]}{\le d}}, \tag{6}$$

a symmetric matrix of order $\sum_{k \le d} \binom{n}{k}$. This is the moment matrix of order d of a $0/1$ problem in the sense of Lasserre [6] and Laurent [7], with f_w playing the role of the (signed) moment sequence. Note that the vertex-weight coordinates w and the moment coordinates f_w are related by the invertible upper-set transform, so any $f : 2^{[n]} \to \mathbb{R}$ is f_w for exactly one w.

3. The vertex dual

Theorem 3.1 (vertex dual)**.** *Let $n, d \in \mathbb{N}$ and $w : 2^{[n]} \to \mathbb{R}$.*

(i) *$L_w(q \cdot (x_i - x_i^2)) = 0$ for every $q \in \mathbb{R}[x]$ and every $i \in [n]$.*

(ii) *Suppose $f_w(\emptyset) = 1$ and that there are $R \in \mathbb{N}$, reals $\lambda_0, \dots, \lambda_{R-1} \ge 0$ and vectors $u_0, \dots, u_{R-1} \in \mathbb{R}^{2^{[n]}}$ such that*

$$f_w(S \cup T) = \sum_{r<R} \lambda_r \, u_r(S) \, u_r(T) \qquad \text{for all } S, T \in \tbinom{[n]}{\le d}, \tag{7}$$

i.e. $M_d(f_w) = \sum_{r<R} \lambda_r u_r u_r^{\mathsf{T}} \succeq 0$ with an explicit decomposition. Then every $c \in \mathcal{F}_{n,d}$ satisfies $c \ge -f_w([n])$.

Proof. (i) Each generator vanishes at every $0/1$ point, $g_i(1_A) = 1_A(i) - 1_A(i)^2 = 0$, so every term $w_A \, q(1_A) \, g_i(1_A)$ of $L_w(qg_i)$ is zero.

(ii) Let $q \in \mathbb{R}[x]$ have total degree at most d, and for $S \subseteq [n]$ let $m_q(S)$ be the sum of the coefficients of the monomials of q with support exactly S. Then $q(1_A) = \sum_{S \subseteq A} m_q(S)$, and $m_q(S) = 0$ unless $|S| \le d$, because a monomial of degree $\le d$ has support of size $\le d$. Expanding q^2 and regrouping by support,

$$L_w(q^2) = \sum_{S,T \in \binom{[n]}{\le d}} m_q(S) \, m_q(T) \, f_w(S \cup T) = \sum_{r<R} \lambda_r \Big(\sum_{S \in \binom{[n]}{\le d}} m_q(S) \, u_r(S) \Big)^2 \;\ge\; 0$$

by (7). Hence $L_w(\sigma_0) \ge 0$ for every $\sigma_0 \in \Sigma_d$. Now let $c \in \mathcal{F}_{n,d}$, say $x_1 \cdots x_n + c = \sigma_0 + \sum_i \sigma_i g_i$ with $\sigma_0 \in \Sigma_d$ and $\sigma_i \in \Sigma_{d-1}$. Applying L_w and using (i), $L_w(x_1 \cdots x_n + c) = L_w(\sigma_0) \ge 0$; and $L_w(x_1 \cdots x_n + c) = f_w([n]) + c \, f_w(\emptyset) = f_w([n]) + c$. □

The multipliers σ_i play no role in the proof, which is why the relaxation is blind to the difference between the quadratic module and the preordering (Polak's Lemma 6.1) and to the Boolean ideal I_n, all of whose elements vanish at every vertex.

In every instance below the weighting is symmetric, $w_A = b_{|A|}$, so $f_w(S) = a_{|S|}$ with $a_k = \sum_{j \ge k} \binom{n-k}{j-k} b_j$, and the moment matrix $\big(a_{|S \cup T|}\big)_{|S|,|T| \le d}$ depends on the $n+1$ numbers $a_0, \dots, a_n$. Optimizing $-a_n$ subject to $a_0 = 1$ and $M_d \succeq 0$ is a semidefinite program in $n+1$ unknowns, and it is exactly the right-hand side of

Polak's formula (2) with $y_k = a_k$. (Symmetrization loses nothing: the objective and the constraints of the relaxation are S_n-invariant and the feasible set is convex.)

Corollary 3.2 (integer certificates)**.** *Let α, β, ℓ be positive integers, let $b_0, \dots, b_n$ and $a_0, \dots, a_n$ be integers, $\mu_0, \dots, \mu_{R-1}$ nonnegative integers and $u_0, \dots, u_{R-1}$ integer vectors indexed by $2^{[n]}$, such that*

(a) $\alpha \sum_{A \supseteq S} b_{|A|} = \beta\, a_{|S|}$ *for every $S \subseteq [n]$ (the upper-set transform of b/β is a/α);*
(b) $a_0 = \alpha$ *(normalization $f(\emptyset) = 1$);*
(c) $\ell\, a_{|S \cup T|} = \alpha \sum_{r<R} \mu_r\, u_r(S)\, u_r(T)$ *for all $S, T \in \binom{[n]}{\le d}$.*

Then every $c \in \mathcal{F}_{n,d}$ satisfies $c \ge -a_n/\alpha$.

Proof. Apply Theorem 3.1 to $w_A = b_{|A|}/\beta$, $\lambda_r = \mu_r/\ell$ and the vectors u_r. □

The hypotheses (a)–(c) are finitely many integer identities and inequalities, so a concrete certificate is verified by evaluation; every lower bound in this paper is an instance of Corollary 3.2, and (a)–(c) for the tabulated data is exactly what the proof assistant checks.

Remark 3.3 (range of the method). If $d \ge n$ then $[n] \in \binom{[n]}{\le d}$ is itself an index of $M_d(f_w)$, so positive semidefiniteness forces $f_w([n]) \ge 0$ and the bound of Theorem 3.1 is at most 0, hence vacuous. This is why the four cells $(2, 2d)$, $2d \ge 4$, of Polak's Table 1 are out of reach of the vertex dual. In the range $d < n$ the relaxation is nontrivial, and Section 5 records where it is and is not tight.

4. Exact values

The dual data of all six lower bounds is collected in Table 2; all of it was found by solving the $(n+1)$-variable semidefinite program of Section 3 numerically, recognizing the optimal a-vector as a vector of small rationals, and verifying positive semidefiniteness of the resulting rational moment matrix by an exact LDL^{T} factorization, which supplies the rank-one decomposition (7). In every case the moment matrix is singular, i.e. the certificate lies on the boundary of the positive semidefinite cone: with $a_0, \dots, a_{n-1}$ held fixed, pushing a_n by one part in a thousand further negative destroys positive semidefiniteness (checked in exact arithmetic at all six cells), so none of the values is a slack certificate that happened to round to a pretty number.

4.1. $n = 2$.

Proposition 4.1. $1/8$ *is the least element of $\mathcal{F}_{2,1}$; that is, $C_2 = 1/8$.*

Proof. Membership is De Klerk and Laurent's identity (1), with $\sigma_0 = \frac{1}{2}(x_1 + x_2 - \frac{1}{2})^2 = \frac{1}{8}(1 - 2x_1 - 2x_2)^2 \in \Sigma_1$ and $\sigma_1 = \sigma_2 = \frac{1}{2} \in \Sigma_0$. The lower bound is Corollary 3.2 with the first line of Table 2: the 3×3 moment matrix $\big(a_{|S \cup T|}\big)_{|S|,|T| \le 1}$ with $a = (1, \frac{1}{4}, -\frac{1}{8})$ is positive semidefinite of rank 2. □

This proposition is routine (a published identity plus a 3×3 check); it is recorded because Polak presents optimality at $n = 2$ only as a case of a numerically supported conjecture, so even this statement is not literally in print.

n	$2d$	certificate data	order	rank
2	2	$b/\beta = (3,3,-1)/8$, $a/\alpha = (8,2,-1)/8$	3	2
4	4	$b/\beta = (3,1,1,3,-1)/24$, $a/\alpha = (24,12,6,2,-1)/24$	11	10
4	6	$b/\beta = (15,15,15,15,-1)/224$, $a/\alpha = (224,104,44,14,-1)/224$	15	14
6	6	$b/\beta = (21,7,0,0,7,21,-6)/288$ $a/\alpha = (288,176,120,78,43,15,-6)/288$	42	27
6	8	$b/\beta = (95,57,19,19,57,95,-7)/2520$ $a/\alpha = (2520,1380,810,468,240,88,-7)/2520$	57	56
6	10	$b/\beta = (63,63,63,63,63,63,-1)/3968$ $a/\alpha = (3968,1952,944,440,188,62,-1)/3968$	63	62

TABLE 2. The vertex-dual certificates: the weight of a vertex 1_A is $b_{|A|}/\beta$ with $b = (b_0,\dots,b_n)$, the moment $f_w(S)$ is $a_{|S|}/\alpha$ with $a = (a_0,\dots,a_n)$, and the last two columns give the order $\sum_{k\le d}\binom{n}{k}$ and the rank of the moment matrix $M_d(f_w)$. The bound is $C_{n,2d} \ge -a_n/\alpha$.

4.2. $n = 4$, $2d = 4$.

Theorem 4.2. $1/24$ *is the least element of* $\mathcal{F}_{4,2}$*; that is,* $C_4 = 1/24$*, and the De Klerk–Laurent value* $1/(n(n+2))$ *is optimal at* $n = 4$.

Proof. Membership is the certificate Polak extracts from his symmetry-reduced semidefinite program [2, Example 2.3 and §3.3], divided by 24:

$$24\,x_1x_2x_3x_4 + 1 = \sigma_0 + \sum_{i=1}^{4}\sigma_i(x_i - x_i^2),$$

with

$$\begin{aligned}\sigma_0 &= \Big(1 + 2\sum_{i<j}x_ix_j - \sum_i x_i^2 - \sum_i x_i\Big)^2 + \Big(\sum_i x_i^2 - \sum_i x_i\Big)^2 \\ &\quad + 2\sum_{i<j}\big(x_i^2 - x_j^2 - x_i + x_j\big)^2,\\ \sigma_i &= 2\Big(1 - x_i - \tfrac12\sum_{j\ne i}x_j\Big)^2 + 6\Big(x_i - \tfrac12\sum_{j\ne i}x_j\Big)^2 \qquad (i\in[4]),\end{aligned}$$

all sums over $[4]$. Here $\sigma_0 \in \Sigma_2$ and $\sigma_i \in \Sigma_1$, as (3) requires with $d = 2$. The identity was expanded in exact rational arithmetic and then re-derived inside the proof assistant. The lower bound is Corollary 3.2 with the second line of Table 2: the 11×11 moment matrix with $a = (1, \frac12, \frac14, \frac{1}{12}, -\frac{1}{24})$ is positive semidefinite of rank 10. □

4.3. $n = 4$, $2d = 6$ **and** $n = 6$, $2d = 6$**: large Gram certificates.** For the remaining two exact values the membership half is no longer a human-readable identity. In both cases it is an exact rational Gram certificate

$$(8)\quad x_1\cdots x_n + C = [x]_d^{\mathsf T} Q\,[x]_d + \sum_{i=1}^{n}\Big((i\,n)\cdot[x]_{d-1}^{\mathsf T} R\,[x]_{d-1}\Big)(x_i - x_i^2), \quad Q\succeq 0,\ R\succeq 0,$$

in the symmetry-reduced form of Polak's Corollary 2.2: $[x]_k$ is the column of all monomials of degree at most k, Q is an S_n-invariant Gram matrix for σ_0, and one

Gram matrix R, invariant under the stabilizer of n, is moved onto the generator g_i by the transposition $(i\ n)$. The matrices were obtained as follows. Solving Polak's block-reduced program numerically reproduces his printed values 0.004464286 and 0.020833333. Complementary slackness against the exact dual of Table 2 (the moment sequence $y_\alpha = a_{|\operatorname{supp}\alpha|}$) forces $Q\,M_d(y) = 0$; imposing these equations together with the coefficient-matching equations as an exact rational affine system, rounding the numerical solution and projecting back onto the affine set keeps the solution inside the optimal face, where positive semidefiniteness survives the rounding. Positive semidefiniteness of Q and R and the identity (8) were then verified in exact rational arithmetic. The resulting sizes are

n	$2d$	C	Q (order, rank)	R (order, rank)
4	6	1/224	35, 21	15, 15
6	6	1/48	84, 57	28, 28

For the machine check each Gram matrix is written as a weighted sum of integer squares, $A\cdot Q = \sum_r \mu_r v_r v_r^{\mathsf{T}}$ with $\mu_r \geq 0$ and v_r integral, by a fraction-free (Bareiss) symmetric elimination; a single positive integer A clears all denominators, and the checked statement is the integer polynomial identity

$$A\,(224\,x_1x_2x_3x_4 + 1) = \sum_r \mu_r\,(v_r\cdot[x]_3)^2 + \sum_{i=1}^{4}\Big(\sum_r \mu_{i,r}\,(v_{i,r}\cdot[x]_2)^2\Big)(x_i - x_i^2) \tag{9}$$

at $(4,6)$, and its analogue with $48\,x_1\cdots x_6 + 1$ at $(6,6)$. The number A has 339 decimal digits at $(4,6)$ and 2032 at $(6,6)$; the sums have 21 and 4×15 squares, respectively 57 and 6×28 squares. The size of A is structural rather than an artefact: the optimal face is thin, and no rounding denominator below 3600 (respectively 10^4) leaves Q positive semidefinite. (A plain rational LDL^{T} factorization of the same Q, which compounds denominators at every pivot, gave a common denominator of more than 1000 digits at $(4,6)$; Bareiss elimination gives 339.)

The certificate and its checker. The membership halves of the two exact values are verified by a certificate checker for truncated quadratic modules, which we describe in the terms of (9); the formal statements are in Appendix A. A certificate consists of a positive integer A; a list B of polynomials, the Gram basis of σ_0 (here the monomials of degree ≤ 3); a list of weighted squares (μ_r, v_r) for σ_0, with $\mu_r \geq 0$ integers and v_r integer vectors indexed by B; a list B' of polynomials, the Gram basis of the multipliers (here the monomials of degree ≤ 2); and, for each generator g_i, a list of weighted squares $(\mu_{i,r}, v_{i,r})$ indexed by B'. Polynomials are represented as sparse lists of integer terms. The checker tests that $A > 0$, that every weight μ_r, $\mu_{i,r}$ is nonnegative, and that the identity

$$A\cdot p = \sum_r \mu_r\,(v_r\cdot B)^2 + \sum_i\Big(\sum_r \mu_{i,r}\,(v_{i,r}\cdot B')^2\Big)g_i \tag{10}$$

holds exactly, by normalizing the difference of the two sides to the empty term list; the Gram matrices themselves are never factored inside the checker, which rebuilds $\sum_r \mu_r v_r v_r^{\mathsf{T}}$ in integer arithmetic and expands it against the basis. Its soundness theorem states: if the checker accepts $(A, B, (\mu_r, v_r), B', (\mu_{i,r}, v_{i,r}))$ against p and the generators $g_1, \ldots, g_n$, if every element of B has total degree at most k and every element of B' total degree at most k', then for every positive integer B_0 there are

$\sigma_0 \in \Sigma_k$ and $\sigma_1, \dots, \sigma_n \in \Sigma_{k'}$ with

$$\tfrac{1}{B_0}\, p = \sigma_0 + \sum_{i=1}^{n} \sigma_i\, g_i. \tag{11}$$

The proof divides (10) by AB_0 and reads each weighted sum of squares as a sum of squares of polynomials of the stated degree (with the real square roots $\sqrt{\mu_r/(AB_0)}$); the transfer of the integer identity, which is checked on term lists, to an identity of polynomials rests on the fact that two real polynomials with the same value at every real point are equal. Applied with $p = 224\, x_1x_2x_3x_4 + 1$, $B_0 = 224$, $(k, k') = (3, 2)$ and $g_i = x_i - x_i^2$, (11) is exactly the statement $x_1x_2x_3x_4 + 1/224 \in \mathcal{M}_{4,3}$; the same with $p = 48\, x_1 \cdots x_6 + 1$ and $B_0 = 48$ gives $x_1 \cdots x_6 + 1/48 \in \mathcal{M}_{6,3}$. We stress the shape of the conclusion: nonnegativity of $x_1 \cdots x_n + C$ on $[0, 1]^n$ holds already at $C = 0$ and says nothing, whereas (11) is the existential statement (3) with the degree bounds on the multipliers, which is what a Lasserre–Putinar relaxation value is defined by. That the degree hypothesis excludes something is verified separately (Proposition 6.1(v)). The representation of a sum of squares by a positive semidefinite Gram matrix over a monomial basis is the standard one, see e.g. Laurent's survey [8].

Theorem 4.3 (membership at $(4, 6)$)**.** *$x_1x_2x_3x_4 + \frac{1}{224} \in \mathcal{M}_{4,3}$; that is, $C_{4,6} \le 1/224$.*

Proof. The identity (9), with A of 339 digits and the $21 + 4 \times 15$ weighted squares described above over the monomials of degree ≤ 3 and ≤ 2, is accepted by the checker; the soundness theorem with $B_0 = 224$ and $(k, k') = (3, 2)$ gives $x_1x_2x_3x_4 + 1/224 = \sigma_0 + \sum_{i=1}^{4} \sigma_i(x_i - x_i^2)$ with $\sigma_0 \in \Sigma_3$ and $\sigma_i \in \Sigma_2$, which is membership in $\mathcal{M}_{4,3}$ by (3). The check itself is an exhaustive integer computation: 39 225 multiply-accumulates of integers of up to 339 digits to rebuild the Gram matrices, then 2 125 monomial products and one normalization of the resulting term list. □

In the formal development this theorem and the exact value that follows from it are the declarations (namespace `Cert.SparsePolyExamples`; `Feas 4 3` is $\mathcal{F}_{4,3}$ of (4))

```
theorem mem_feas_4_3 : (1/224 : ℝ) ∈ HypercubeSosConst.Feas 4 3
theorem C46_eq : IsLeast (HypercubeSosConst.Feas 4 3) (1/224 : ℝ)
```

Theorem 4.4. *$1/224$ is the least element of $\mathcal{F}_{4,3}$; that is, $C_{4,6} = 1/224$. In particular Polak's suggested value at $(n, 2d) = (4, 6)$ is the exact value.*

Proof. Lower bound: Corollary 3.2 with the third line of Table 2; the 15×15 moment matrix with $a = (1, \frac{13}{28}, \frac{11}{56}, \frac{1}{16}, -\frac{1}{224})$ is positive semidefinite of rank 14. Upper bound: Theorem 4.3. □

Theorem 4.5 (membership at $(6, 6)$)**.** *$x_1x_2 \cdots x_6 + \frac{1}{48} \in \mathcal{M}_{6,3}$; that is, $C_6 \le 1/48$.*

Proof. The $(6, 6)$ analogue of (9), with A of 2032 digits and the $57 + 6 \times 28$ weighted squares over the monomials of degree ≤ 3 and ≤ 2 in six variables, is accepted by the checker (the six multiplier lists are the images of one list of 28 squares under the transpositions $(i\ 6)$, as in (8)); the soundness theorem with $B_0 = 48$ and $(k, k') = (3, 2)$ gives membership in $\mathcal{M}_{6,3}$. The check is 533 904 integer multiply-accumulates at 2032-digit weights followed by 11 760 monomial products; at this size it is delegated to compiled code (Section 6). □

In the formal development this theorem and the exact value that follows are

```
theorem mem_feas_6_3 : (1/48 : ℝ) ∈ HypercubeSosConst.Feas 6 3
theorem C6_eq : IsLeast (HypercubeSosConst.Feas 6 3) (1/48 : ℝ)
```

Theorem 4.6. $1/48$ *is the least element of* $\mathcal{F}_{6,3}$*; that is,* $C_6 = 1/48$*, and the De Klerk–Laurent value* $1/(n(n+2))$ *is optimal at* $n = 6$*.*

Proof. Lower bound: Corollary 3.2 with the fourth line of Table 2; the 42×42 moment matrix with $a = (1, \frac{11}{18}, \frac{5}{12}, \frac{13}{48}, \frac{43}{288}, \frac{5}{96}, -\frac{1}{48})$ is positive semidefinite of rank 27. Upper bound: Theorem 4.5. □

De Klerk and Laurent verified $n = 6$ by computer only ("using computer for $n = 4, 6$", §1.2), so even the upper bound $C_6 \le 1/48$ had not been certified before. That the $n = 6$ certificate is so much larger than the $n = 4$ one is not an artefact of the solver. Since every multiplier term vanishes at the vertices, σ_0 takes the value C at each vertex 1_A with $A \neq [n]$ and $C + 1$ at $1_{[n]}$. At $n = 2$ and $n = 4$ these are the vertex values of a single square of a polynomial of degree d in $e_1 = \sum_i x_i$, because $1 + a^2 \prod_{k=0}^{n-1}(t-k)$ is a perfect square in t for a suitable a ($(2t-1)^2$ with $a^2 = 4$, and $(t^2 - 3t + 1)^2$ with $a^2 = 1$): De Klerk and Laurent's σ_0 is $\frac{1}{8}(2e_1 - 1)^2$, and at $n = 4$ the first square of Polak's σ_0 agrees with $24\,x_1x_2x_3x_4 + 1$ at every vertex (his two further groups of squares are needed for the identity to hold as polynomials; in fact no certificate at $(4, 4)$ has $\sigma_0 = \frac{1}{24}(e_1^2 - 3e_1 + 1)^2$, since the multiplier Gram matrix this σ_0 forces, which is unique, is not positive semidefinite). At $n = 6$, by contrast, $1 + \frac{1}{15}\prod_{k=0}^{5}(t-k)$ factors as $\frac{1}{15}(t^2 - 5t + 1)(t^4 - 10t^3 + 34t^2 - 45t + 15)$ and is not a square, so not even the vertex values of σ_0 can be those of a single square of a polynomial in e_1.

5. Lower bounds at $(6, 8)$ and $(6, 10)$

Theorem 5.1. *Every* $c \in \mathcal{F}_{6,4}$ *satisfies* $c \ge 1/360$*; that is,* $C_{6,8} \ge 1/360$*.*

Proof. Corollary 3.2 with the fifth line of Table 2: the 57×57 moment matrix with $a = (1, \frac{23}{42}, \frac{9}{28}, \frac{13}{70}, \frac{2}{21}, \frac{11}{315}, -\frac{1}{360})$ is positive semidefinite of rank 56. The rank-one decomposition (7) produced by the exact LDL^{T} of this boundary matrix has a common denominator of 80 decimal digits over 56 terms. □

Polak's numerical value at $(6, 8)$ is 0.002777778 and his suggested value is $1/360 = 0.002\overline{7}$. We prove only the lower half; the matching Gram certificate would be the analogue of Section 4.3 with Q of order $\binom{10}{4} = 210$, and we have not constructed it.

Theorem 5.2. *Every* $c \in \mathcal{F}_{6,5}$ *satisfies* $c \ge 1/3968$*; that is,* $C_{6,10} \ge 1/3968$*.*

Proof. Corollary 3.2 with the last line of Table 2: the 63×63 moment matrix with $a = (1, \frac{61}{124}, \frac{59}{248}, \frac{55}{496}, \frac{47}{992}, \frac{1}{64}, -\frac{1}{3968})$ is positive semidefinite of rank 62. The rank-one decomposition has a common denominator of 30 decimal digits over 62 terms. □

This bound is deliberately recorded although it is *not* tight: the bound $1/3968$ equals $0.000252016\ldots$, while Polak's numerical value of $C_{6,10}$ is 0.000310382. It is the datum that fixes where the vertex dual stops being tight. Summarizing the measured range (the comparison with Polak's numerical values is a numerical observation, not a theorem): the exact optimum of the relaxation of Section 3 equals the numerical $C_{n,2d}$ to all nine printed decimals at $(2, 2)$, $(4, 4)$, $(4, 6)$, $(6, 6)$,

$(6,8)$ and $(8,8)$, i.e. at every cell of Polak's table with $d < n$ and $2d \le n+2$, and it is strictly smaller at $(6,10)$, where $2d = n+4$.

Remark 5.3 (the relaxation at $d = n-1$; not part of the formal development). The three cells $(2,2)$, $(4,6)$, $(6,10)$ have $d = n-1$, and in all three the optimal weighting in Table 2 is flat: $w_A = t$ for $A \neq [n]$ and $w_{[n]} = -s$. For such a weighting $f_w(S) = t(2^{\,n-|S|}-1) - s$, so $M_{n-1}(f_w) = t\,G - (t+s)\,\mathbf{1}\mathbf{1}^{\mathsf T}$ with $G_{S,T} = 2^{\,n-|S\cup T|}$. Here $G = VV^{\mathsf T}$ for the $(2^n-1)\times 2^n$ matrix $V_{S,A} = [S \subseteq A]$, whose rows are linearly independent, and $\mathbf{1} = Ve_{[n]}$; so $\mathbf{1}^{\mathsf T}G^{-1}\mathbf{1}$ is the squared norm of the projection of $e_{[n]}$ onto the row space of V, whose orthogonal complement in $\mathbb{R}^{2^n}$ is spanned by the single vector $\nu_A = (-1)^{n-|A|}$, whence $\mathbf{1}^{\mathsf T}G^{-1}\mathbf{1} = 1-2^{-n}$. Thus $M_{n-1}(f_w) \succeq 0$ iff $(t+s)(1-2^{-n}) \le t$, and maximizing s under $f_w(\emptyset) = 2^n t - t - s = 1$ gives $s = 1/(2^n(2^n-2))$, at $t = (2^n-1)/(2^n(2^n-2))$. By Theorem 3.1 the flat weightings alone therefore give $C_{n,2(n-1)} \ge 1/(2^n(2^n-2))$ for every $n \ge 2$. This is also the exact optimum of the relaxation, for every n: the polynomial $q = (-1)^n\big(\prod_i(1-2x_i) - (-2)^n x_1\cdots x_n\big)$ has degree $n-1$, takes the value $(-1)^{n-|A|}$ at every vertex 1_A with $A \neq [n]$ and $-(2^n-1)$ at $1_{[n]}$, and so satisfies $q^2 = 1 + 2^n(2^n-2)\,x_1\cdots x_n$ at every vertex, i.e. $x_1\cdots x_n + 1/(2^n(2^n-2)) \equiv \big(q/\sqrt{2^n(2^n-2)}\big)^2 \pmod{I_n}$; applying L_w to this congruence as in Remark 5.4 below gives $-f_w([n]) \le 1/(2^n(2^n-2))$ for every feasible w. The value is $1/8$, $1/224$, $1/3968$ at $n = 2,4,6$: the true $C_{n,2(n-1)}$ at $n = 2,4$, and not at $n = 6$. (At $n = 2$ the square is De Klerk and Laurent's $\frac{1}{8}(1-2x_1-2x_2)^2$.) This is a pen-and-paper argument, checked in exact arithmetic for $n \le 7$; it is not formalized and no theorem depends on it.

Remark 5.4 (Polak's Problem 1; derived in prose, not formalized). The proof of Theorem 3.1(ii) uses only that every generator vanishes at every vertex; every element of the Boolean ideal I_n has the same property. Hence if $x_1\cdots x_n + C \equiv \sum_j q_j^2 \pmod{I_n}$ with $\deg q_j \le d$, and w is as in Theorem 3.1(ii), then $L_w(x_1\cdots x_n + C) = \sum_j L_w(q_j^2) \ge 0$, so $C \ge -f_w([n])$; that is, the vertex dual bounds Polak's $C^{\mathrm{bool}}_{n,2d}$ from below by the same numbers as $C_{n,2d}$. Together with Polak's Lemma 6.1, $C^{\mathrm{bool}}_{n,2d} \le C_{n,2d}$, and the exact values of Proposition 4.1 and Theorems 4.2, 4.4, 4.6, this gives

$$C^{\mathrm{bool}}_{2,2} = C_2 = \tfrac{1}{8}, \quad C^{\mathrm{bool}}_{4,4} = C_4 = \tfrac{1}{24}, \quad C^{\mathrm{bool}}_{6,6} = C_6 = \tfrac{1}{48}, \quad C^{\mathrm{bool}}_{4,6} = C_{4,6} = \tfrac{1}{224},$$

so the answer to Problem 1 of [2] is affirmative for $n = 2,4,6$, and the analogous equality holds at the off-diagonal cell $(4,6)$. At $(6,10)$, on the other hand, the single Boolean square of Remark 5.3 gives $C^{\mathrm{bool}}_{6,10} \le 1/3968$, while Polak's numerical value of $C_{6,10}$ is $0.000310382 > 1/3968$; so, numerically, the equality does not extend to $2d = n+4$ (the exact value of $C_{6,10}$ is not known). The Boolean arguments in this remark are not part of the formal development.

6. Verification

All theorems and propositions of Sections 3–5 are stated and proved in Lean 4 (version 4.32.0) against Mathlib [10, 11]; the exact statements are reproduced verbatim in Appendix A, and the repository reference is to be added at submission. The definitions (3) and (4) are `QM n d` and `Feas n d` on Mathlib's `MvPolynomial (Fin n) ℝ`, and an exact value $C_{n,2d} = v$ is the statement `IsLeast (Feas n d) v`. Nothing in the development is assumed: no `sorry`, no added `axiom`.

The vertex dual. Theorem 3.1 is `Lw_mul_gen` (part (i)) and `le_of_feas` (part (ii)); Corollary 3.2 is `Cert.bound`, whose hypothesis `Cert.ok` is a decidable predicate on the integer tables of Table 2 (with the vectors u_r stored as integer lists indexed by the bitmask of S). These three declarations depend only on the standard axioms `propext`, `Classical.choice`, `Quot.sound` of Mathlib; no computation is involved.

Lower bounds. Each of the six instances discharges `Cert.ok` on its data by evaluation. At $(2,2)$, $(4,4)$, $(4,6)$ and $(6,6)$ this is done by the kernel (`decide`), so `C2_eq`, `C4_eq`, `le_of_feas_4_3` and `le_of_feas_6_3` carry only the three standard axioms. At $(6,8)$ and $(6,10)$ the rank-one decompositions have 80- and 30-digit common denominators over 56 and 62 terms, and the check is delegated to compiled code (`native_decide`); the theorems `le_of_feas_6_4` and `le_of_feas_6_5` therefore each carry one additional axiom, the trust in the compiled evaluation of their own certificate (`le_of_feas_6_4._native.native_decide.ax_1_1` and the analogue for `6_5`). The reduction they rest on is kernel-checked in every case.

Upper bounds. The identities (1) and the $n = 4$ certificate of Theorem 4.2 are proved by `ring` after extensionality (`mem_feas_2`, `mem_feas_4`). The two large identities of Section 4.3 (Theorems 4.3 and 4.5) are checked by the certificate checker of Section 4.3: a polynomial is reflected as a sparse list of integer terms, the right-hand side of (9) is rebuilt from the weighted integer squares in integer arithmetic, and the identity becomes a single Boolean, `QMCert.check gens cert target = true`, whose soundness theorem `qmCheck_sound` (Appendix A) is the statement (11): it produces membership in $\mathcal{M}_{n,d}$ with the degree bounds *on the multipliers*, the sums-of-squares statement `SOSdeg` being written in exactly the shape of `IsSOS`. The transfer from term lists to `MvPolynomial` is the evaluation map together with extensionality of polynomials over the infinite field $\mathbb{R}$. The technique itself is prior art: Li, Xiong and Yang [9] verify an exact constrained sum-of-squares certificate in Lean 4 by reflecting the polynomial as a sparse type and comparing normal forms under `native_decide`; their conclusion is nonnegativity on a simplex. At $(4,6)$ the check (`check46`: 39 225 integer multiply-accumulates at up to 339 digits, then 2 125 monomial products) runs in the kernel in about 90 seconds, so `mem_feas_4_3` and `C46_eq` carry only the three standard axioms. At $(6,6)$ (`check66`: 533 904 multiply-accumulates at 2032 digits) the kernel evaluation was still running after 11 minutes at 15 GB and was abandoned, so `check66` is a `native_decide` statement and `mem_feas_6_3`, `C6_eq` carry the single additional axiom `check66._native.native_decide.ax_1_1`.

Axiom summary. Every declaration named in this paper depends on `propext`, `Classical.choice` and `Quot.sound` only, with exactly three exceptions, each of which adds the single `native_decide` axiom of one certificate evaluation: the lower bounds of Theorems 5.1 and 5.2 (`le_of_feas_6_4` and `le_of_feas_6_5`) and the upper half of Theorem 4.6 (`check66`, hence Theorem 4.5, i.e. `mem_feas_6_3`, and `C6_eq`). In particular $C_4 = 1/24$ and $C_{4,6} = 1/224$ are checked by the kernel throughout. The list was produced by `#print axioms` on 2026-09-03 and is reproduced in Appendix A; for this version the axioms of the declarations of Theorems 4.3, 4.4, 4.5, 4.6 and of Proposition 6.1 were re-read (same day, same output).

Controls. A checker that is a decidable predicate must be shown to refuse something, or the membership statements would be vacuous. The following proposition is not a new result; it is recorded because it is what protects Theorems 4.3 and 4.5 from being empty.

Proposition 6.1 (controls)**.** *Let $\mathcal{C}_2$ be the certificate data of* (1) *in its integer form* $8x_1x_2 + 1 = (1 - 2x_1 - 2x_2)^2 + 4g_1 + 4g_2$*, i.e.* $A = 1$*,* $B = (1, x_1, x_2)$*, the single weighted square* $(1, (1, -2, -2))$*,* $B' = (1)$ *and the multiplier squares* $(4, (1))$ *for* g_1 *and for* g_2*, which the checker accepts against* $8x_1x_2 + 1$*. The checker refuses each of the following corruptions of* $\mathcal{C}_2$*:*

(i) *the same data against the target* $9x_1x_2 + 1$ *(a too-small constant: the certificate does not prove* $x_1x_2 + 1/9 \in \mathcal{M}_{2,1}$*);*
(ii) *the scale* $A = 2$ *in place of* $A = 1$*;*
(iii) *the square vector* $(1, -2, -3)$ *in place of* $(1, -2, -2)$*;*
(iv) *the weight* -1 *in place of* $+1$ *on the square of* σ_0*.*

Moreover

(v) *the degree hypothesis of the soundness theorem is not vacuous: the Gram basis* $B = (1, x_1, x_2)$ *of* $\mathcal{C}_2$ *fails the degree-*0 *test, while the multiplier basis* $B' = (1)$ *passes it, which is exactly the pair of degree bounds* $\mathcal{M}_{2,1}$ *asks for.*

Proof. Each item is the evaluation of a decidable predicate on three-monomial data, performed by the kernel (`decide`). In the names of Appendix A, (i)–(iv) are

`check_ne_wrong_constant`, `check_ne_wrong_scale`,
`check_ne_perturbed_square`, `check_ne_negative_weight`

(and their `= false` forms, named `control_wrong_constant` and so on), and (v) is

`basisDegOK_ne_trivial`, `control_degree_not_vacuous`, `control_degree_multiplier`.

In (iv) the weight test of the checker, which is the nonnegativity hypothesis of the soundness theorem, is a conjunct separate from the identity test; the corrupted datum fails both tests. □

On the dual side, the statements `IsLeast` carry their own control: a value smaller than the one proved is refuted by the certificate, a larger one by the membership.

Published material re-derived. The two identities the source prints, De Klerk and Laurent's (1) and the $n = 4$ certificate of [2, Example 2.3], were expanded in exact rational arithmetic and re-proved inside the proof assistant (`mem_feas_2`, `mem_feas_4`), including the degree conditions; both are correct as printed. Polak's numerical values at the six cells of Table 1 were reproduced to the nine decimals he prints by an independent implementation of his block-reduced program before any value was claimed.

Appendix A. The Lean statements

The statements are quoted verbatim from the development; proof terms are omitted. The common prefix `LeanProblemSpec.` of all namespaces is dropped, the namespace is `HypercubeSosConst` unless noted, `n` is an implicit natural number and `X i` is the i-th variable; line breaks were adjusted to the page width.

Definitions (`Defs.lean`).

```
noncomputable def gen (n : ℕ) (i : Fin n) : MvPolynomial (Fin n) ℝ := X i - X i ^ 2

def IsSOS (k : ℕ) (σ : MvPolynomial (Fin n) ℝ) : Prop :=
  ∃ (m : ℕ) (q : Fin m → MvPolynomial (Fin n) ℝ),
    (∀ j, (q j).totalDegree ≤ k) ∧ σ = ∑ j, q j ^ 2

def QM (n d : ℕ) : Set (MvPolynomial (Fin n) ℝ) :=
  {p | ∃ (σ₀ : MvPolynomial (Fin n) ℝ) (σ : Fin n → MvPolynomial (Fin n) ℝ),
```

```
      IsSOS d σ₀ ∧ (∀ i, IsSOS (d - 1) (σ i)) ∧ p = σ₀ + ∑ i, σ i * gen n i}

noncomputable def tgt (n : ℕ) (c : ℝ) : MvPolynomial (Fin n) ℝ :=
  (∏ i, X i) + MvPolynomial.C c

def Feas (n d : ℕ) : Set ℝ := {c : ℝ | tgt n c ∈ QM n d}

def vpt (A : Finset (Fin n)) : Fin n → ℝ := fun i => if i ∈ A then 1 else 0

noncomputable def Lw (w : Finset (Fin n) → ℝ) (p : MvPolynomial (Fin n) ℝ) : ℝ :=
  ∑ A : Finset (Fin n), w A * eval (vpt A) p

noncomputable def fw (w : Finset (Fin n) → ℝ) (S : Finset (Fin n)) : ℝ :=
  ∑ A : Finset (Fin n), w A * (if S ⊆ A then 1 else 0)

def Sd (n d : ℕ) : Finset (Finset (Fin n)) := univ.filter (fun S => S.card ≤ d)
```

Theorem 3.1 and Corollary 3.2 (`Defs.lean`; `c : Cert n d` is the integer data of Corollary 3.2 and `c.ok` its conditions (a)–(c)).

```
lemma Lw_mul_gen (w : Finset (Fin n) → ℝ) (q : MvPolynomial (Fin n) ℝ) (i : Fin n) :
    Lw w (q * gen n i) = 0

theorem le_of_feas {d R : ℕ} (w : Finset (Fin n) → ℝ)
    (lam : ℕ → ℝ) (u : ℕ → Finset (Fin n) → ℝ)
    (hlam : ∀ r, 0 ≤ lam r)
    (hdec : ∀ S ∈ Sd n d, ∀ T ∈ Sd n d,
        fw w (S ∪ T) = ∑ r ∈ Finset.range R, lam r * u r S * u r T)
    (hone : fw w ∅ = 1)
    {c : ℝ} (hc : c ∈ Feas n d) : - fw w univ ≤ c

theorem bound (h : c.ok) {x : ℝ} (hx : x ∈ Feas n d) :
    -((c.al.getD n 0 : ℝ) / (c.aden : ℝ)) ≤ x
```

Proposition 4.1, Theorem 4.2 (`Small.lean`).

```
theorem mem_feas_2 : (1/8 : ℝ) ∈ Feas 2 1
theorem C2_eq : IsLeast (Feas 2 1) (1/8 : ℝ)
theorem mem_feas_4 : (1/24 : ℝ) ∈ Feas 4 2
theorem C4_eq : IsLeast (Feas 4 2) (1/24 : ℝ)
```

Lower halves of Theorems 4.4, 4.6, 5.1, 5.2 (`N4Deg6.lean`, `N6Deg6.lean`, `N6Deg8.lean`, `N6Deg10.lean`).

```
theorem le_of_feas_4_3 {c : ℝ} (hc : c ∈ Feas 4 3) : (1/224 : ℝ) ≤ c
theorem le_of_feas_6_3 {c : ℝ} (hc : c ∈ Feas 6 3) : (1/48 : ℝ) ≤ c
theorem le_of_feas_6_4 {c : ℝ} (hc : c ∈ Feas 6 4) : (1/360 : ℝ) ≤ c
theorem le_of_feas_6_5 {c : ℝ} (hc : c ∈ Feas 6 5) : (1/3968 : ℝ) ≤ c
```

The certificate checker.
Namespace `Cert.SparsePoly`. Here `Poly` is a list of integer terms, `toP n` is its image in `MvPolynomial (Fin n) ℝ`, `basisDegOK k` tests that every basis polynomial has degree at most `k`, and `QMCert.check gens c p` is the Boolean described in Section 6 (positivity of `c.den`, nonnegativity of every weight, and the integer identity (9) tested by normalizing a term list to zero).

```
def SOSdeg (n k : ℕ) (σ : MvPolynomial (Fin n) ℝ) : Prop :=
  ∃ (m : ℕ) (q : Fin m → MvPolynomial (Fin n) ℝ),
    (∀ j, (q j).totalDegree ≤ k) ∧ σ = ∑ j, q j ^ 2

theorem qmCheck_sound (n k k' : ℕ) (gens : List Poly) (c : QMCert) (p : Poly)
    (hlen : gens.length = n)
    (hb0 : basisDegOK k c.basis0 = true) (hbM : basisDegOK k' c.basisM = true)
    (B : Int) (hB : 0 < B)
    (h : QMCert.check gens c p = true) :
    ∃ (σ₀ : MvPolynomial (Fin n) ℝ) (σ : Fin n → MvPolynomial (Fin n) ℝ),
      SOSdeg n k σ₀ ∧ (∀ i, SOSdeg n k' (σ i)) ∧
        C (((B : ℝ))⁻¹) * toP n p
          = σ₀ + ∑ i : Fin n, σ i * toP n (gens.getD (i : ℕ) [])
```

Upper halves and exact values of Theorems 4.4 and 4.6.
Namespace `Cert.SparsePolyExamples`; here `hcGens n` is the list of the g_i, `tgt46` the term list of $224x_1x_2x_3x_4+1$, `tgt66` that of $48x_1\cdots x_6+1$, and `cert46`, `cert66` the certificate data.

```
theorem check46 : QMCert.check (hcGens 4) cert46 tgt46 = true
theorem mem_feas_4_3 : (1/224 : ℝ) ∈ HypercubeSosConst.Feas 4 3
theorem C46_eq : IsLeast (HypercubeSosConst.Feas 4 3) (1/224 : ℝ)
theorem check66 : QMCert.check (hcGens 6) cert66 tgt66 = true
theorem mem_feas_6_3 : (1/48 : ℝ) ∈ HypercubeSosConst.Feas 6 3
theorem C6_eq : IsLeast (HypercubeSosConst.Feas 6 3) (1/48 : ℝ)
```

Controls (Proposition 6.1).
Namespaces `HypercubeSosConst.Exact` (the `≠` forms) and `Cert.SparsePolyExamples` (the `= false` forms and the last two); here `cert2` and `tgt2` are the data of (1) in its integer form $8x_1x_2+1=(1-2x_1-2x_2)^2+4g_1+4g_2$, and `check2` is the acceptance.

```
theorem check2 : QMCert.check (hcGens 2) cert2 tgt2 = true

theorem check_ne_wrong_constant :
    QMCert.check (hcGens 2) cert2 [(9, List.replicate 2 1), (1, List.replicate 2 0)]
      ≠ true
theorem check_ne_wrong_scale :
    QMCert.check (hcGens 2) { cert2 with den := 2 } tgt2 ≠ true
theorem check_ne_perturbed_square :
    QMCert.check (hcGens 2) { cert2 with sqs0 := [(1, [1, -2, -3])] } tgt2 ≠ true
theorem check_ne_negative_weight :
    QMCert.check (hcGens 2) { cert2 with sqs0 := [(-1, [1, -2, -2])] } tgt2 ≠ true
theorem basisDegOK_ne_trivial : basisDegOK 0 cert2.basis0 ≠ true

theorem control_wrong_constant :
    QMCert.check (hcGens 2) cert2 [(9, List.replicate 2 1), (1, List.replicate 2 0)]
      = false
theorem control_perturbed_square :
    QMCert.check (hcGens 2) { cert2 with sqs0 := [(1, [1, -2, -3])] } tgt2 = false
theorem control_negative_weight :
    QMCert.check (hcGens 2) { cert2 with sqs0 := [(-1, [1, -2, -2])] } tgt2 = false
theorem control_wrong_scale :
    QMCert.check (hcGens 2) { cert2 with den := 2 } tgt2 = false
theorem control_degree_not_vacuous : basisDegOK 0 cert2.basis0 = false
theorem control_degree_multiplier : basisDegOK 0 cert2.basisM = true
```

Axioms, as printed by `#print axioms` on 2026-09-03 (re-read for this version on the same day with identical output). The abbreviation `std` stands for the three standard axioms `propext`, `Classical.choice` and `Quot.sound`.

```
Lw_mul_gen, le_of_feas, Cert.bound, mem_feas_2, C2_eq, mem_feas_4, C4_eq,
  le_of_feas_4_3, le_of_feas_6_3, qmCheck_sound, mem_feas_4_3, C46_eq   std
le_of_feas_6_4            std, le_of_feas_6_4._native.native_decide.ax_1_1
le_of_feas_6_5            std, le_of_feas_6_5._native.native_decide.ax_1_1
check66                   propext, check66._native.native_decide.ax_1_1
mem_feas_6_3, C6_eq       std, check66._native.native_decide.ax_1_1
check46, check_ne_wrong_constant, check_ne_wrong_scale,
  check_ne_perturbed_square, check_ne_negative_weight,
  control_wrong_constant, control_wrong_scale,
  control_perturbed_square, control_negative_weight            propext
basisDegOK_ne_trivial, control_degree_not_vacuous,
  control_degree_multiplier                                    (none)
```

References

[1] E. de Klerk and M. Laurent, Error bounds for some semidefinite programming approaches to polynomial minimization on the hypercube, *SIAM J. Optim.* 20 (2010), no. 6, 3104–3120, DOI 10.1137/100790835.

[2] S. Polak, Sum-of-squares certificates for symmetric polynomials on the hypercube: a counterexample to a conjecture of De Klerk and Laurent, arXiv:2605.31169v1 [math.OC], 29 May 2026.

[3] L. Baldi and L. Slot, Degree bounds for Putinar's Positivstellensatz on the hypercube, *SIAM J. Appl. Algebra Geom.* 8 (2024), no. 1, 1–25, DOI 10.1137/23M1555430; arXiv:2302.12558.

[4] S. Gribling, E. de Klerk and J. Vera, Revisiting the convergence rate of the Lasserre hierarchy for polynomial optimization over the hypercube, *Optimization* (2026), 1–28, DOI 10.1080/02331934.2026.2641624; arXiv:2505.00544.

[5] S. Gribling, E. de Klerk and J. C. Vera, Squared polynomial approximation kernels for the hypercube: improved error bounds and implications for Lasserre hierarchies, arXiv:2605.31496v1 [math.OC], 29 May 2026.

[6] J. B. Lasserre, Global optimization with polynomials and the problem of moments, *SIAM J. Optim.* 11 (2001), no. 3, 796–817, DOI 10.1137/S1052623400366802.

[7] M. Laurent, A comparison of the Sherali–Adams, Lovász–Schrijver, and Lasserre relaxations for 0–1 programming, *Math. Oper. Res.* 28 (2003), 470–496, DOI 10.1287/moor.28.3.470.16391.

[8] M. Laurent, Sums of squares, moment matrices and optimization over polynomials, in *Emerging Applications of Algebraic Geometry* (M. Putinar and S. Sullivant, eds.), IMA Vol. Math. Appl. 149, Springer, New York, 2009, 157–270, DOI 10.1007/978-0-387-09686-5_7.

[9] J. Li, B. Xiong and Z. Yang, A proof of the Dittert conjecture in dimension 4 via an exact constrained sum-of-squares certificate, arXiv:2607.29191v2 [cs.SC], 10 August 2026.

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

[11] L. de Moura and S. Ullrich, The Lean 4 theorem prover and programming language, in *Automated Deduction – CADE 28*, LNCS, Springer, 2021, 625–635, DOI 10.1007/978-3-030-79876-5_37.