Quadratic Refinements in Combinatorial Games: Impartial Realization, Gold Forms, and Coherence Limits

GPT 5.6 Sol Claude Fable 5 a9lim

Abstract

Let Q be a quadratic refinement of an alternating form on a finite $\mathbb{F}_2$-space. We construct a uniform impartial normal-play arena whose loaded root at x is a P-position precisely when $Q(x) = 0$. Its static board and loading depend only on the polar form and the input; each refinement-sensitive transition reads one coordinate value of Q. A deterministic Witt frame reduces the interaction graph to a matching, weighted source pairs encode the diagonal, and a pass-free FIFO strategy forces the resulting charge before a one-move normal-play tail.

The observation cost is optimal. Every exact transcript-stable rule must query directions spanning x, and weight-w queries therefore require at least $\lceil \mathrm{wt}(x)/w \rceil$ observations; block compression attains this bound. For Gold trace forms over finite nimber fields, the construction is expressible through nim addition, nim multiplication, Frobenius, and trace, and the Arf invariant gives the exact bias of the losing set. The same trace monomial defines a central Gold–Heisenberg extension whose squares and commutators recover the quadratic and polar forms; at trace-one scale over $\mathbb{F}_4$, this extension is the quaternion group Q_8.

We also place the construction between two sharp boundaries. A single partizan selector decodes every $\mathbb{Z}/4$-valued Brown refinement through its four outcome classes, whereas any coefficient-faithful Clifford datum coherent on all short-game values vanishes on torsion and collapses over the usual coefficient rings. The finite realization and these boundary theorems are formalized in Lean.

1 Introduction

Classical impartial constructions realize linear losing sets: coin turning decomposes into nim heaps, kernels of Grundy maps produce codes, and lexicographic codes admit game-theoretic models [4, 10, 14]. The linearity is forced, not incidental: nim values of coin-turning games add coin-wise [4], so the P-positions of every such game form an $\mathbb{F}_2$-linear code, the starting point of the codes-from-games program of [10, 14]. More generally, impartial P/N recursion can emulate arbitrary Boolean update rules in modular and invariant heap games [19]; there the Boolean function is compiled into the rules, and which losing sets admit *invariant* rules is subtle already in the linear world [12]. Binary quadratic forms also organize the orbit structure of lit-only sigma-games on nondegenerate graphs [17], but those are configuration-reachability puzzles rather than alternating normal-play realizations. We study a different quadratic analogue. Given a quadratic refinement Q of an alternating binary form, the objective is a single uniform normal-play rule whose losing loadings are exactly the quadric $\{x : Q(x) = 0\}$.

Uniformity needs an information model. An arbitrary finite set could be declared terminal in a purpose-built acyclic graph, so the arena here is required to be independent of the refinement and every access to Q is counted. The construction uses one singleton query per refinement-sensitive transition. Its complete query set is also optimal: exactness forces the observed directions to span the input. The resulting statement is the following.

Theorem A (Theorems 4.2 and 5.2 with Corollary 5.3)**.** *Fix an alternating bilinear form B on a finite-dimensional $\mathbb{F}_2$-space and an input x. There is one impartial normal-play arena, with board and loading built from B and x alone, in which each refinement-sensitive transition reads the single coordinate value $Q(e_j)$ of a loaded source, and whose loaded root is a P-position exactly when $Q(x) = 0$, simultaneously for every quadratic refinement Q of B. Conversely, every exact transcript-stable rule observes directions spanning x; observations of coordinate weight at most w therefore number at least $\lceil \mathrm{wt}(x)/w \rceil$, and block compression attains this bound at every width.*

The principal examples are the Gold trace forms

$$Q_a(x) = \mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(x^{1+2^a}).$$

When $\mathbb{F}_{2^m}$ is identified with a finite nimber subfield, addition, multiplication, Frobenius, and trace are all built from nim operations [9, 20]. Gold monomials originate in sequence design [15]. Their trace components are binary quadratic forms, whose polar ranks and Walsh spectra have been studied by quadratic-form and Weil-sum methods [11, 16, 18]. The realization therefore connects normal-play outcomes directly to Arf statistics and to a trace-defined central extension.

Sections 3–4 define the access model and prove the realization theorem. Section 5 establishes the sharp observation lower bound. Sections 6 and 7 specialize the construction to Gold forms. The Brown selector of Section 8 extends the outcome encoding from one bit to $\mathbb{Z}/4$, while Section 9 proves the obstruction to extending such finite constructions coherently across all short games.

Only matching-plus-isolates boards occur in the proof. The arbitrary-graph isolated-dummy FIFO conjecture is strictly stronger and plays no role in the realization theorem.

2 Quadratic and game-theoretic preliminaries

2.1 Quadratic refinements

Let V be an m-dimensional $\mathbb{F}_2$-space. A quadratic refinement of an alternating bilinear form B is a function $Q : V \to \mathbb{F}_2$ such that

$$Q(x + y) = Q(x) + Q(y) + B(x, y).$$

For fixed B, the refinements form a torsor under V^*: every other refinement has the form $Q + \ell$ for a unique linear functional ℓ.

If B is nonsingular and $(a_i, b_i)_{i=1}^r$ is a symplectic basis, the Arf invariant is

$$\mathrm{Arf}(Q) = \sum_{i=1}^{r} Q(a_i)Q(b_i) \in \mathbb{F}_2.$$

It classifies nonsingular binary quadratic forms at fixed dimension [3, 13]. Their zero count is

$$\#\{x : Q(x) = 0\} = 2^{2r-1} + (-1)^{\mathrm{Arf}(Q)}2^{r-1}.$$

For a degenerate form of polar rank $2r$ on an m-dimensional space, the values are balanced when Q is nonzero on $\operatorname{rad} B$. If $Q|_{\operatorname{rad} B} = 0$, the count is

$$2^{m-1} + (-1)^{\mathrm{Arf}(Q_{\mathrm{ns}})}2^{m-r-1},$$

where Q_{ns} is the nonsingular quotient.

Fix an ordered basis $e_1, \dots, e_m$. Put

$$P_B(z) = \sum_{j<k} B(e_j, e_k) z_j z_k, \qquad q_j = Q(e_j).$$

Then

$$Q(z) = P_B(z) + \sum_j q_j z_j.$$

The alternating form is public data; the diagonal vector (q_j) is the additional information carried by the refinement.

2.2 Normal-play semantics

A finite impartial normal-play position is a P-position when the previous player wins, equivalently when the player to move has no winning move. The four outcome classes of a finite partizan game are denoted $\mathcal{N}, \mathcal{P}, \mathcal{L}, \mathcal{R}$: respectively the next player, previous player, Left, or Right wins. We use only ordinary Conway equality and normal-play outcomes [9, 4].

3 The access model

Definition 3.1 (Local realization)**.** Fix the ordered coordinate frame of V. A local realization of quadratic refinements has the following data and properties.

1. The alternating form B, the input x, and the coordinate frame are public. The refinement is accessed through queries $Q(z)$.
2. The position set, loading map, terminal set, and declared outcome convention are independent of Q.
3. Each move predicate and transition together make at most c adaptive queries, each at a vector of coordinate weight at most w_0, where c, w_0 are independent of m.
4. For every refinement Q of every admitted B, the loaded root at x has the target outcome if and only if $Q(x) = 0$.

The definition controls local access but intentionally does not define an informal notion of "natural game." Section 5 gives the representation-invariant information lower bound that follows from exactness, and also explains why a generic fork-based liveness test cannot do more.

4 The weighted-source Witt–FIFO arena

4.1 Public adapted coordinates

Use deterministic Gaussian elimination to choose a basis $f_1, \dots, f_m$ depending only on B. It consists of symplectic pairs and radical vectors, and its only nonzero pairings are

$$B(f_{a_h}, f_{b_h}) = 1.$$

Write

$$f_i = \sum_j C_{ji} e_j, \qquad x = \sum_i y_i f_i, \qquad p_i = P_B(f_i).$$

All of C, y, and p_i are public. Expanding the quadratic form in the adapted basis and using the coordinate formula above gives the identity

$$Q(x) = \sum_i y_i p_i + \sum_j x_j q_j + \sum_h y_{a_h} y_{b_h}.$$

Indeed,

$$Q(x) = \sum_i y_i Q(f_i) + \sum_h y_{a_h} y_{b_h}, \qquad Q(f_i) = p_i + \sum_j C_{ji} q_j,$$

and $\sum_i y_i C_{ji} = x_j$.

4.2 The arena

Load one strategic coin F_i for each $y_i = 1$. Join F_{a_h} to F_{b_h} when both are loaded; these edges have weight 1. For each coordinate with $x_j = 1$, also load a source pair S_j^0, S_j^1 whose edge has weight $q_j = Q(e_j)$. The *potential matching* contains every such strategic and source edge, even when its actual weight is zero. Hence the matching is independent of Q.

A core state is $(U, \mathcal{Q}, k, \sigma)$, where U is the untouched set, $\mathcal{Q}$ is a FIFO queue of open coins, $k \in \mathbb{F}_2$ is a one-step ko bit, and $\sigma \in \mathbb{F}_2$ is the accumulated charge. Initially every loaded coin is untouched, the queue is empty, and $k = \sigma = 0$. The position universe contains coherent states for both values of σ, whether or not both are reachable for a given refinement.

There are two impartial moves.

- OPEN(v) removes v from U and appends it to the queue. If its potential mate is already in the queue, the edge weight is added to σ. Opening into an empty queue sets ko; every other opening clears it.
- CLOSE removes the queue front. It is legal when the queue is nonempty and either ko is clear or U is empty. Closing a strategic coin F_i adds p_i to σ; all other closes have zero charge.

There is no pass. Every coin is opened once and later closed once. The quantity

$$2|U| + |\mathcal{Q}|$$

decreases by one on every move, and the exhausted-board exception to ko ensures that the core never stalls before drainage. Thus every core play has exactly two moves per loaded coin.

At a drained state, add one move to an optionless sink exactly when $\sigma = 1$. This tail is impartial and reads only the stored charge, not the refinement oracle.

4.3 The matching strategy

For a queue front f, call an opponent checkpoint *safe* when either ko protects f or its potential mate is not untouched. Equivalently, every legal close has zero degree from f into U in the public matching.

Theorem 4.1 (Public matching strategy)**.** *For a finite matching plus isolates, either designated seat has a deterministic strategy, depending only on the public matching and order, that makes every close have zero public live degree. Consequently the touch intervals of the endpoints of every matched edge overlap.*

Proof. Fix a public order. While U is nonempty, the designated seat never closes. If the queue is empty, it opens the least untouched coin. Otherwise, it opens the untouched mate of the front when that mate exists, and the least untouched coin when it does not. Once U is empty, it closes.

Induct on the displayed clock. Opening into an empty queue sets ko, so the opponent receives a safe checkpoint. If the front's mate is untouched, opening it erases the front's only possible live neighbour. If no mate is untouched, opening any coin preserves that fact. Thus every move of the designated seat hands the opponent a safe checkpoint. At such a checkpoint, a close, if legal, has live degree zero. An opening returns the turn with the same queue front; the designated seat then opens that front's untouched mate if necessary, restoring safety. When U is empty, every close has live degree zero. This proves the claim for either initial seat.

If the endpoints of an edge did not overlap, the first endpoint opened would close while its mate remained untouched, giving live degree one. The strategy excludes this possibility. □

Under the FIFO discipline closes occur in opening order, so two touch intervals never nest: they are disjoint or they interlace. The overlap forced by Theorem 4.1 therefore makes every matched pair an interlaced chord in the chord diagram of the play; compare the interlacement and isotropic-systems framework of [5].

Theorem 4.2 (Quadratic realization)**.** *The weighted-source Witt–FIFO arena is a local impartial realization with $(w_0, c) = (1, 1)$. For every alternating form B, every quadratic refinement Q, and every input x, its loaded root is a P-position if and only if $Q(x) = 0$.*

Proof. Apply Theorem 4.1 to the full public potential matching. The same strategy works for every assignment of source-edge weights. Every strategic edge and every source pair overlaps, so their total opening charge is

$$\sum_h y_{a_h} y_{b_h} + \sum_j x_j q_j.$$

Every active strategic coin closes exactly once, contributing $\sum_i y_i p_i$. By the adapted-coordinate identity, either designated seat therefore forces the drained charge to equal $Q(x)$.

The core has even length, so after drainage it is the first player's turn. If $Q(x) = 1$, the first player uses the public strategy, reaches charge one, and takes the tail move. If $Q(x) = 0$, the second player uses the same strategy and leaves the first player at an optionless drained state. Hence the root is N in the first case and P in the second.

All static data use only B, x, and the fixed frame. A source opening makes at most the single query $Q(e_j)$ and every other transition is refinement-blind. The arena therefore satisfies Definition 3.1 with $(w_0, c) = (1, 1)$. □

The theorem is a strategy statement. It does not claim that every off-policy play drains with charge $Q(x)$. It also does not use a theorem for arbitrary graphs: deterministic Witt reduction produces exactly the matching class of Theorem 4.1.

5 The observation boundary

We now measure the complete set of refinement observations that determines a rooted outcome, allowing the set to be chosen adaptively.

Definition 5.1 (Transcript stability)**.** Let $S(Q, x) \subset V$ be a finite set of observed directions and let $R(Q, x)$ be the rooted result. The observation interface is *transcript-stable* if

$$Q(z) = Q'(z) \text{ for all } z \in S(Q, x) \quad \Longrightarrow \quad R(Q, x) = R(Q', x)$$

for every two refinements Q, Q' of the same polar form.

Theorem 5.2 (Span lower bound)**.** *Suppose the rooted result is transcript-stable and exact at x for the full torsor of refinements of B. Then*

$$x \in \operatorname{span} S(Q, x).$$

If every observed vector has coordinate weight at most w, then

$$|S(Q, x)| \geq \left\lceil \frac{\operatorname{wt}(x)}{w} \right\rceil.$$

In particular, no constant total number of bounded-weight observations gives an exact family in unbounded dimension.

Proof. If $x \notin \operatorname{span} S$, finite-dimensional separation supplies a linear functional ℓ vanishing on S with $\ell(x) = 1$. Then Q and $Q + \ell$ give the same observation transcript and hence the same rooted result, while their target bits at x differ. This contradicts exactness.

For the coordinate bound, vectors of weight at most w cover at most $|S|w$ coordinates. Their span cannot contain x unless their union covers the support of x. Therefore $\operatorname{wt}(x) \leq |S|w$. □

Viewed on the affine torsor, the observations are adaptive linear, or parity, queries in the sense of parity decision trees [27]. The theorem is the usual annihilator argument for the linear torsor of quadratic refinements, transported to adaptive transcripts; compare also the linear-structures framework for Boolean functions in [8].

Corollary 5.3 (Attainment at every width)**.** *Fix $w \geq 1$. There is a local realization whose distinct observations at x are exactly $\lceil \operatorname{wt}(x)/w \rceil$ vectors of weight at most w. Hence the lower bound of Theorem 5.2 is sharp.*

Proof. Partition $\operatorname{supp}(x)$ into disjoint nonempty blocks $Z_1, \ldots, Z_k$ of size at most w, where $k = \lceil \operatorname{wt}(x)/w \rceil$, and let z_i be their indicator vectors. Define $L : \mathbb{F}_2^k \to V$ by $L(e'_i) = z_i$, and pull back the quadratic form:

$$Q' = Q \circ L, \qquad B'(u, v) = B(Lu, Lv).$$

Then Q' is a quadratic refinement of B' and $Q'(\mathbf{1}) = Q(z_1 + \cdots + z_k) = Q(x)$. Apply Theorem 4.2 to the induced instance at $\mathbf{1}$, answering its singleton query $Q'(e'_i)$ with the original-frame query $Q(z_i)$. The blocks are disjoint, linearly independent, and sum to x, so the resulting observation set has exactly the asserted size and weights. □

The access model cannot, by itself, make an outcome-only definition of "strategically non-evaluative." The following generic obstruction rules out one tempting test.

Proposition 5.4 (Fork padding)**.** *Every finite normal-play tree can be padded, without changing its root outcome, so that every completed play enters an unavoidable two-action fork whose unique winning action depends on a chosen bit. Thus the existence of a reachable, optimal, or unavoidable refinement-sensitive winning fork does not certify non-evaluative behavior.*

Proof. Take a two-option N-position in which exactly one option is P, and exchange the two options when the chosen bit changes. Replace every original terminal P-node by a one-option wrapper whose child is this fork. The wrapper remains P, so backward induction preserves every ancestor outcome, while every original complete play now reaches the bit-sensitive fork. □

6 Gold trace forms

Let $K_m = \mathbb{F}_{2^m}$ and let $\mathrm{Tr}_m : K_m \to \mathbb{F}_2$ be absolute trace. For $a \geq 0$ and $c \in K_m$, define

$$Q_{a,c}(x) = \mathrm{Tr}_m(cx^{1+2^a}), \qquad Q_a = Q_{a,1}.$$

We call $Q_{a,c}$ a scaled Gold trace form, using "Gold" for the monomial shape without imposing the APN convention $\gcd(a, m) = 1$. Its polar form is

$$B_{a,c}(x, y) = \mathrm{Tr}_m\big(c(xy^{2^a} + yx^{2^a})\big).$$

When K_m is identified with a finite nimber subfield, all operations in these formulas are nimber operations. The quadratic-tower construction below uses the canonical subfields of power-of-two degree. Every field-theoretic claim is internal to the displayed K_m; no algebraic-closure property is used.

6.1 The all-exponent diagonal source

Choose a basis $e_0, \ldots, e_{m-1}$ of K_m over $\mathbb{F}_2$ with $e_0 = 1$. Nondegeneracy of the trace pairing gives a unique diagonal dual $\lambda_{a,c}^{(m)} \in K_m$ satisfying

$$\mathrm{Tr}_m(\lambda_{a,c}^{(m)} e_i) = \mathrm{Tr}_m(ce_i e_i^{2^a}) \qquad (0 \leq i < m).$$

Thus $\lambda_{a,c}^{(m)}$ packages the entire basis diagonal into one trace-linear field element. This is structural compression specific to the Gold datum, not a contradiction of the full-torsor observation lower bound of Section 5.

Theorem 6.1 (Diagonal source criterion)**.** *For every m, a, c as above,*

$$\mathrm{Tr}_m(\lambda_{a,c}^{(m)}) = \mathrm{Tr}_m(c), \qquad \lambda_{a,c}^{(m)} \in \{w^2 + w : w \in K_m\} \iff \mathrm{Tr}_m(c) = 0.$$

In particular, if $m \geq 2$ is even and $c = 1$, there is a $w_a^{(m)} \in K_m$ such that

$$Q_a(e_i) = \mathrm{Tr}_m\big((w_a^{(m)})^2 + w_a^{(m)})e_i\big) \quad (0 \leq i < m).$$

Proof. Set $e_0 = 1$ in the defining trace-duality identity. This gives $\mathrm{Tr}_m(\lambda_{a,c}^{(m)}) = \mathrm{Tr}_m(c)$. In a finite field of characteristic 2, the image of $w \mapsto w^2 + w$ is exactly the kernel of absolute trace [21, Theorem 2.25]. This proves the equivalence. For $c = 1$ and even m, $\mathrm{Tr}_m(1) = 0$. □

The source can be constructed recursively in a quadratic tower. Write $K_{2M} = K_M(u) = K_M \oplus uK_M$ with conjugation $\sigma(u) = u + 1$. Relative trace satisfies

$$(1 + \sigma)((A + uB)e) = Be, \qquad (1 + \sigma)((A + uB)ue) = (A + B)e.$$

Consequently, if $e_j^{*,(M)}$ is trace-dual to e_j in K_M, then

$$e_{M+j}^{*,(2M)} = e_j^{*,(M)}, \qquad e_j^{*,(2M)} = (1 + u)e_j^{*,(M)}.$$

These identities give a closed recursion for $\lambda_{a,c}^{(2M)}$ from its two diagonal blocks.

Likewise, if $u^2 + u = \delta$ with $\mathrm{Tr}_M(\delta) = 1$ and $\lambda = A + uB$ has trace zero, seek $w = X + uY$. Then

$$w^2 + w = (X^2 + X + \delta Y^2) + u(Y^2 + Y).$$

First solve $Y^2 + Y = B$. The two choices Y and $Y + 1$ toggle the trace of $A + \delta Y^2$, so exactly one makes the second downstairs equation $X^2 + X = A + \delta Y^2$ soluble. Iteration constructs a source throughout the quadratic nimber tower. Theorem 6.1 is not a claim that an arbitrary scaled component has such a source: the exact obstruction is $\mathrm{Tr}_m(c)$.

6.2 Arf controls the win bias

Corollary 6.2. *Apply Theorem 4.2 to Q_a on K_m. Its P-loadings are exactly the Gold quadric $\{x : Q_a(x) = 0\}$. If the polar rank is $2r$ and Q_a vanishes on its radical, then*

$$\#P - 2^{m-1} = (-1)^{\mathrm{Arf}((Q_a)_{\mathrm{ns}})} 2^{m-r-1}.$$

If Q_a is nonzero on the radical, the two outcomes are balanced.

Proof. The realization theorem identifies P-positions with zeros of Q_a. The nonsingular and radical zero-count formulas above give the stated census. □

For the unscaled Gold form,

$$\operatorname{rad} B_a = \mathbb{F}_{2^{\gcd(2a,m)}}, \qquad \operatorname{rank} B_a = m - \gcd(2a, m),$$

by trace adjointness and the fixed-field equation $x^{2^{2a}} = x$; this is the standard Gold rank calculation [11, 16]. Thus the rank fixes the possible magnitude of the bias, the restriction to the radical decides whether that bias vanishes, and the Arf class fixes its sign. Parameter-specific Walsh evaluations refine this invariant-level statement.

7 The Gold–Heisenberg extension

The correspondence between binary quadratic forms, central extensions of elementary abelian 2-groups, and extraspecial 2-groups is classical: the square map supplies the quadratic form and commutators supply its polar form [23, Sections 4–5]. Here the oriented Gold trace monomial gives an explicit cocycle.

The same trace monomial defines a structural multiplication without a unary quadratic oracle. Put

$$\phi_{a,c}(x, y) = \mathrm{Tr}_m(cxy^{2^a}), \qquad Q_{a,c}(x) = \phi_{a,c}(x, x).$$

Theorem 7.1 (Gold–Heisenberg group)**.** *On $E_{a,c} = \mathbb{F}_2 \times K_m$, define*

$$(s, x)(t, y) = \big(s + t + \phi_{a,c}(x, y), x + y\big).$$

Then $E_{a,c}$ is a group fitting into a central extension

$$1 \longrightarrow \mathbb{F}_2 \longrightarrow E_{a,c} \longrightarrow K_m^+ \longrightarrow 1.$$

For $z = (1, 0)$,

$$(s, x)^2 = z^{Q_{a,c}(x)},$$
$$[(s, x), (t, y)] = z^{B_{a,c}(x,y)}.$$

Its center is

$$Z(E_{a,c}) = \{(s, r) : s \in \mathbb{F}_2, r \in \operatorname{rad} B_{a,c}\}.$$

Hence it is extraspecial exactly when $B_{a,c}$ is nondegenerate and nonzero.

Proof. The map $\phi = \phi_{a,c}$ is biadditive, so

$$\phi(x, y) + \phi(x + y, w) = \phi(y, w) + \phi(x, y + w),$$

the normalized cocycle identity. It proves associativity of the displayed product. The identity is $(0, 0)$ and $(s, x)^{-1} = (s+Q_{a,c}(x), x)$. Direct substitution gives the square law; swapping two factors changes the central coordinate by $\phi(x, y) + \phi(y, x) = B_{a,c}(x, y)$, proving the commutator law. An element is central precisely when this last value vanishes for every y, which gives the center formula and the extraspecial criterion. □

Corollary 7.2 (Quaternion cell)**.** *Let $K_2 = \mathbb{F}_4$, let $a = 1$, and choose $c \in K_2$ with $\mathrm{Tr}_2(c) = 1$. Then the Gold–Heisenberg extension $E_{1,c}$ is isomorphic to the quaternion group Q_8.*

Proof. Every nonzero $x \in K_2$ satisfies $x^3 = 1$, and therefore

$$Q_{1,c}(x) = \mathrm{Tr}_2(cx^3) = 1.$$

For distinct nonzero x, y, their sum is also nonzero, so $B_{1,c}(x, y) = Q_{1,c}(x+y)+Q_{1,c}(x)+Q_{1,c}(y) = 1$. Thus $B_{1,c}$ is nondegenerate, $E_{1,c}$ has order eight and center $\{1, z\}$, and every noncentral element squares to z. The classification of groups of order eight identifies $E_{1,c}$ with Q_8. □

Every operation in the extension product is expressed on $(s, x) \in \mathbb{F}_2 \times K_m$ by nimber operations: disjunctive sum supplies addition, nim product supplies multiplication, repeated squaring supplies Frobenius, and trace is a finite iterated sum. The multiplication contains neither a table of basis diagonals nor a $Q_{a,c}$ query; its squares reveal the quadratic form because that is the defining structure of the extension. In particular, Corollary 7.2 builds the quaternion group from nim operations alone: a group-level positive answer to the quaternion case of [2, Problem 5.3(j)] inside a finite nimber core, whose value-level ambient counterpart fails by Section 9.

For the unscaled form, put $d = \gcd(2a, m)$ and $R = \mathbb{F}_{2^d} = \mathrm{rad}\, B_a$. If m is a power of two and $d < m$, then m/d is even, so absolute trace vanishes on R. Hence

$$Q_a|_R = 0, \qquad \phi_a|_{R\times R} = 0.$$

The subgroup $\{(0, r) : r \in R\}$ is central, and the quotient is a canonical extraspecial extension of K_m/R of order 2^{1+m-d}. This is a per-field, Frobenius-covariant construction. It is not asserted to be coherent under every inclusion of short-game subgroups; Section 9 shows why that stronger condition would force collapse.

There are now two distinct directions in which to enlarge the finite binary construction. One replaces the coefficient bit by a $\mathbb{Z}/4$-valued refinement while retaining a finite input space. The other asks for one quadratic datum coherent across the full additive group of short games. The next two sections give, respectively, a positive selector and a negative coherence theorem.

8 Brown refinements as partizan outcomes

Let $q : V \to \mathbb{Z}/4$ satisfy

$$q(x + y) = q(x) + q(y) + 2b(x, y),$$

where $b : V \times V \to \mathbb{F}_2$ is symmetric bilinear. Such forms underlie the Brown invariant and the associated fourth-root Gauss sums [6, 7]; their algebraic classification and coding applications are developed in [26, 24].

Proposition 8.1 (Canonical binary split)**.** *There are unique maps $\ell : V \to \mathbb{F}_2$ and $Q : V \to \mathbb{F}_2$ such that*

$$q = \widehat{\ell} + 2Q,$$

where $\widehat{0} = 0$ and $\widehat{1} = 1$ in $\mathbb{Z}/4$. The map ℓ is linear, and Q is a quadratic refinement with polar form

$$B_Q = b + \ell \otimes \ell.$$

Moreover, if $W(R) = \sum_x (-1)^{R(x)}$, then

$$\sum_{x \in V} i^{q(x)} = \frac{1+i}{2} W(Q) + \frac{1-i}{2} W(Q + \ell).$$

Proof. Reduction modulo two gives the linear map $\ell = q \bmod 2$; the second binary digit defines Q. The carry identity $\widehat{r+s} = \widehat{r} + \widehat{s} + 2rs$ gives $B_Q = b + \ell \otimes \ell$. Finally,

$$i^{\ell} = \frac{1+i}{2} + \frac{1-i}{2}(-1)^{\ell},$$

which yields the Walsh decomposition. This is the two-component transform decomposition used for generalized Boolean functions; compare [25, Lemma 17]. □

For an ordinary binary quadratic form R, let $\mathcal{A}_R(x)$ denote the impartial arena of Theorem 4.2. Thus

$$o(\mathcal{A}_R(x)) = \mathcal{P} \quad \Longleftrightarrow \quad R(x) = 0.$$

Theorem 8.2 (Intrinsic Brown selector)**.** *The single partizan game*

$$\mathcal{B}_q(x) = \{\mathcal{A}_{Q+\ell}(x) \mid \mathcal{A}_Q(x)\}$$

has outcome

$q(x)$	0	1	2	3
$o(\mathcal{B}_q(x))$	$\mathcal{N}$	$\mathcal{R}$	$\mathcal{P}$	$\mathcal{L}$.

Hence the fixed decoder $\mathcal{N}, \mathcal{R}, \mathcal{P}, \mathcal{L} \mapsto 0, 1, 2, 3$ recovers $q(x)$.

Proof. The four binary possibilities are

$q(x)$	0	1	2	3
$\ell(x)$	0	1	0	1
$Q(x)$	0	0	1	1
$Q(x) + \ell(x)$	0	1	1	0.

If Left starts, her sole move enters $\mathcal{A}_{Q+\ell}(x)$ with Right to move, so she wins exactly when $Q(x) + \ell(x) = 0$. If Right starts, his sole move enters $\mathcal{A}_Q(x)$ with Left to move, so he wins exactly when $Q(x) = 0$. The two starter bits give the displayed outcomes. □

This is one intrinsic game, not a synchronized product of two arenas: after the root move, play enters exactly one follower. The four-outcome census recovers the correlated Gauss sum in the Walsh decomposition. The selector remains defined when that sum vanishes, although in that case no Brown phase is assigned by Gauss-sum normalization.

9 The ambient-coherent game-exterior obstruction

The additive group of short partizan game values is not a ring under Conway multiplication. Altman and Lipparini ask whether a different game-theoretic product could produce quaternions, octonions, or general Clifford algebras [2, Problem 5.3(j)]. The Gold–Heisenberg extension of Section 7 answers the group-level quaternion fragment positively inside a finite nimber core. We now give a negative result for a precise value-level interpretation on the full short-game group.

Let $\mathcal{S}$ be the additive group of short-game values, R a commutative ring, C an R-algebra, and $\iota : R \hookrightarrow C$ an injective coefficient map. A coefficient-faithful Clifford datum consists of an additive map $j : \mathcal{S} \to C$, a function $Q : \mathcal{S} \to R$, and a function $B : \mathcal{S} \times \mathcal{S} \to R$ satisfying

$$j(x)^2 = \iota(Q(x)), \qquad j(x)j(y) + j(y)j(x) = \iota(B(x,y)).$$

It is *ambient-coherent* when it is defined on all of $\mathcal{S}$; equivalently, compatible data on a cofinal directed family of finitely generated subgroups glue to such a datum.

Theorem 9.1 (Game-exterior obstruction)**.** *In every ambient-coherent coefficient-faithful datum,*

$$Q(x), B(x,y) \in \bigcap_{k \geq 0} 4^k R \qquad (x, y \in \mathcal{S}).$$

For every torsion game t and every $x \in \mathcal{S}$,

$$Q(t) = 0, \qquad B(t,x) = B(x,t) = 0.$$

Thus the quadratic and polar data factor through the torsion-free quotient. In particular, Q and B vanish identically when $R = \mathbb{Z}$, when R has characteristic 2, or when $R = \mathbb{Z}/4$.

Proof. Moews's structure theorem makes $\mathcal{S}$ two-divisible, constructs halves explicitly, and gives only power-of-two finite orders [22, Theorems 8–9]. For every k, write $x = 2^k u$ and $y = 2^k v$. Additivity of j and the defining Clifford identities give

$$Q(x) = 4^k Q(u), \qquad B(x,y) = 4^k B(u,v),$$

where coefficient faithfulness is used to return from C to R.

Now let $nt = 0$, with n a power of two, and choose y with $ny = t$. Since $nj(t) = j(nt) = 0$,

$$j(t)^2 = j(t)j(ny) = (nj(t))j(y) = 0,$$

so $Q(t) = 0$. For arbitrary x, choose z with $nz = x$. Then

$$j(t)j(x) + j(x)j(t) = (nj(t))j(z) + j(z)(nj(t)) = 0,$$

so $B(t,x) = 0$; symmetry gives the reversed value. Polarization now yields $Q(x+t) = Q(x)$, proving factorization of the quadratic data.

Finally, $\bigcap_k 4^k R = 0$ in each named coefficient ring. □

The coherence hypothesis is substantive. A quadratic table on a selected, root-incomplete subgroup is not constrained by a root that lies outside that subgroup. Likewise the Gold forms use the field operations internal to a finite nimber core and are not asserted to extend through all short-game inclusions. The positive finite-field construction and the negative ambient theorem therefore address different naturality conditions.

10 Formal verification and implementation boundary

The Lean development accompanying Ogdoad [1] formalizes the theorem chain at the following boundaries. Its import-only entry point is `Ogdoad.Papers.GoldArf`; shared results remain owned by reusable modules rather than being copied into the paper surface.

- `SymplecticBasis`, `WittFrame`, and `GoldMatchingAlgebra` prove the deterministic orthogonal decomposition, its flattened public matching, and the adapted-coordinate quadratic identity.
- `FifoMatching`, `ImpartialRealizer`, `PhysicalDeferred`, and `GoldArena` prove the safe-front strategy, exact clock and tail, ledger conjugacies, and the literal-root equivalence `gold_literal_root_isP_iff`.
- `GoldNoEvaluator`, `GoldBlockCompression`, and `GoldForkPadding` prove the span lower bound, its sharp block construction, and outcome-preserving fork padding.
- `Algebra.ArtinSchreier`, `GoldDiagonal`, `GoldExtraspecial`, and `GoldExtraspecialTrace` prove the finite-field diagonal source, with the reusable Artin–Schreier trace-kernel and lifting algebra owned by the shared module, the cocycle extension and its trace specialization, and Corollary 7.2 as an explicit group isomorphism over Mathlib's GF(4).
- `BrownGame`, `BrownSelectorPGame`, and `GameExterior` prove the binary Brown split, intrinsic selector, coefficient divisibility, and torsion-collapse consequences.

The literal realization theorem includes the computed Witt basis, transport from the displayed coordinate frame, the OPEN and CLOSE transition rules, a single public policy valid for every source weighting, and the normal-play tail. It is therefore an end-to-end theorem about the concrete loaded root, not merely a collection of algebraic ingredients. The phase-aware compiler in `GoldSemantics.lean` is an independent comparison surface and is not required by this proof.

Two interfaces remain deliberately external. Moews's theorem on the two-divisible, two-primary-torsion structure of the short-game group is a cited hypothesis of the game-exterior formalization. Mathlib's abstract finite fields are not definitionally identified with the Rust finite-nimber backend, so agreement of concrete arithmetic representations is tested rather than assumed in Lean.

Finally, `Fifo.lean` states but does not prove the isolated-dummy FIFO theorem for arbitrary graphs. The present construction uses the proved matching-plus-isolates theorem only; no bounded census or open proposition is a premise of Theorem 4.2.

11 Conclusion

Finite binary quadratic refinements admit a uniform impartial realization with refinement-independent statics and one singleton query per sensitive transition. The construction is exact, and its observation complexity is best possible at every permitted query width. For Gold forms, nimber arithmetic supplies the full datum, the Arf invariant measures the losing-set bias, and the associated trace cocycle realizes the same form through group squares and commutators, with the trace-one $\mathbb{F}_4$ cell equal to Q_8.

The partizan Brown selector and the ambient-coherence obstruction describe the two natural extensions of this result. Modulo 4, one game carries both binary components through its four

outcomes. Across the entire short-game group, however, divisibility and torsion force coefficient-faithful quadratic data to collapse. The resulting picture is therefore sharp: finite-field quadratic structure has an exact game realization, while unrestricted value-level coherence does not.

References

[1] a9lim. Ogdoad: Clifford algebras, quadratic forms, and combinatorial games. GitHub repository, 2026. Formal development under `formal/`; cited at release `v1.0.3`.

[2] Harry Altman and Paolo Lipparini. A ring structure on the class of combinatorial games, 2026.

[3] Cahit Arf. Untersuchungen über quadratische formen in körpern der charakteristik 2, teil i. *Journal für die reine und angewandte Mathematik*, 183:148–167, 1941.

[4] Elwyn R. Berlekamp, John H. Conway, and Richard K. Guy. *Winning Ways for your Mathematical Plays*. Academic Press, London, 1982.

[5] Robert Brijder and Lorenzo Traldi. Isotropic matroids II: Circle graphs. *Electronic Journal of Combinatorics*, 23(4):#P4.2, 2016. arXiv:1504.04299.

[6] Edgar H. Brown, Jr. Generalizations of the Kervaire invariant. *Annals of Mathematics*, 95:368–383, 1972.

[7] Gregory W. Brumfiel and John W. Morgan. Quadratic functions, the index modulo 8, and a $\mathbb{Z}/4$-Hirzebruch formula. *Topology*, 12(2):105–122, 1973.

[8] Claude Carlet. *Boolean Functions for Cryptography and Coding Theory*. Cambridge University Press, 2021.

[9] John H. Conway. *On Numbers and Games*. Academic Press, London, 1976.

[10] John H. Conway and Neil J. A. Sloane. Lexicographic codes: Error-correcting codes from game theory. *IEEE Transactions on Information Theory*, 32(3):337–348, 1986.

[11] Robert S. Coulter. On the evaluation of a class of Weil sums in characteristic 2. *New Zealand Journal of Mathematics*, 28(2):171–184, 1999.

[12] Eric Duchêne, Aline Parreau, and Michel Rigo. Deciding game invariance. *Information and Computation*, 253:127–142, 2017. arXiv:1408.5274.

[13] Richard Elman, Nikita Karpenko, and Alexander Merkurjev. *The Algebraic and Geometric Theory of Quadratic Forms*, volume 56 of *Colloquium Publications*. American Mathematical Society, 2008.

[14] Aviezri S. Fraenkel. Error-correcting codes derived from combinatorial games. In Richard J. Nowakowski, editor, *Games of No Chance*, volume 29 of *MSRI Publications*, pages 417–431. Cambridge University Press, 1996.

[15] Robert Gold. Maximal recursive sequences with 3-valued recursive cross-correlation functions. *IEEE Transactions on Information Theory*, 14(1):154–156, 1968.

[16] Tor Helleseth and P. Vijay Kumar. Sequences with low correlation. In Vera S. Pless and W. Cary Huffman, editors, *Handbook of Coding Theory*, volume 2, pages 1765–1853. Elsevier, Amsterdam, 1998.

[17] Hau-wen Huang. Lit-only sigma-game on nondegenerate graphs. *Journal of Algebraic Combinatorics*, 41(2):385–395, 2015.

[18] Jyrki Lahtonen, Gary McGuire, and Harold N. Ward. Gold and Kasami–Welch functions, quadratic forms, and bent functions. *Advances in Mathematics of Communications*, 1(2):243–250, 2007.

[19] Urban Larsson and Johan Wästlund. From heaps of matches to the limits of computability. *Electronic Journal of Combinatorics*, 20(3):P41, 2013.

[20] H. W. Lenstra, Jr. Nim multiplication. *Séminaire de Théorie des Nombres de Bordeaux*, 7, 1977–1978. Exposé 11, pp. 1–24.

[21] Rudolf Lidl and Harald Niederreiter. *Finite Fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, 2nd edition, 1997.

[22] David Moews. The abstract structure of the group of games. In Richard J. Nowakowski, editor, *More Games of No Chance*, volume 42 of *MSRI Publications*, pages 49–57. Cambridge University Press, 2002.

[23] Daniel Quillen. The mod 2 cohomology rings of extra-special 2-groups and the spinor groups. *Mathematische Annalen*, 194(3):197–212, 1971.

[24] Kai-Uwe Schmidt. $\mathbb{Z}_4$-valued quadratic forms and quaternary sequence families. *IEEE Transactions on Information Theory*, 55(12):5803–5810, 2009.

[25] Pantelimon Stănică, Thor Martinsen, Sugata Gangopadhyay, and Brajesh Kumar Singh. Bent and generalized bent boolean functions. *Designs, Codes and Cryptography*, 69(1):77–94, 2013.

[26] Jay A. Wood. Witt's extension theorem for mod four valued quadratic forms. *Transactions of the American Mathematical Society*, 336(1):445–461, 1993.

[27] Zhiqiang Zhang and Yaoyun Shi. On the parity complexity measures of boolean functions. *Theoretical Computer Science*, 411(26–28):2612–2618, 2010.