# The Complexity of Oracle-Efficient Realizable Transductive Learning

Changlong Wu
University of Arizona
clwu@arizona.edu

**Abstract**

In realizable transductive online learning, the learner knows the entire sequence of $T$ instances in advance, and the labels are consistent with one of $N$ hypotheses. With explicit access to the hypothesis class, the halving algorithm makes at most $\log_2 N$ mistakes. *Can a comparable guarantee be achieved using only polynomially many empirical risk minimization (ERM) queries?* We answer this question negatively, even for a weighted-ERM oracle that optimizes arbitrary real-valued linear objectives and returns a complete maximizing hypothesis. For every fixed $\beta \in (0, 1)$ and every randomized learner making polynomially many oracle queries, there exists a fixed realizable instance with exactly $N = 2^{\lfloor T^\beta \rfloor}$ hypotheses on which the learner makes $\Omega_\beta(\sqrt{T \log N})$ mistakes in expectation. This matches the agnostic-rate upper bound achieved by random playout using $O(T)$ oracle calls. The separation persists for much smaller classes as well: along a sequence with $\log N = \Theta((\log T)^2)$, we establish a mistake lower bound of $\exp(\Omega(\log T / \log \log T))$. Our main technical contribution is a *composition lemma* that combines two realizable prediction problems such that their mistake lower bounds add, up to a small loss, while their hypothesis class sizes grow only additively. Iterating this lemma yields a family of hard instances spanning the desired parameter regimes, establishing a sharp separation between information-theoretic and oracle-efficient mistake guarantees.

## 1 Introduction

In transductive online learning, the learner knows the entire instance sequence $x_1, \ldots, x_T$, but not the labels (Ben-David et al., 1997; Kakade and Kalai, 2005). On each round $t$, the learner predicts a binary label $\hat{y}_t$ for $x_t$ and then observes the true label $y_t$. A *hypothesis class* $\mathcal{H}$ specifies the candidate labelings of these instances. Since the instance sequence is fixed, we may identify each hypothesis with its *trace*, the corresponding $T$-bit label vector. We therefore work directly with a finite class $\mathcal{H} \subseteq \{0, 1\}^T$ of size $N$. The label sequence is *realizable* if it coincides with some $h^\star \in \mathcal{H}$, which we call the *target trace*.

In the realizable setting, the *halving algorithm* (Barzdin and Freivald, 1972; Littlestone, 1988) achieves a mistake upper bound of $\log_2 N$. It predicts the majority label among hypotheses consistent with the labels observed so far. Each mistake eliminates at least half of these hypotheses, yielding the logarithmic upper bound. The challenge is its computation: implementing the majority prediction requires counting, or at least comparing the numbers of, consistent hypotheses supporting each label. This can be difficult when the hypothesis class is large and represented implicitly.

A natural approach to computational efficiency is to replace explicit operations over the hypothesis class with calls to an *optimization oracle* (Kalai and Vempala, 2005; Dudík et al., 2020). Empirical risk minimization (ERM) is a particularly natural choice: it is fundamental to supervised learning and underlies many oracle-efficient online-learning algorithms (Kakade and Kalai, 2005; Cesa-Bianchi and Shamir, 2013; Wang et al., 2022). For parameterized models, ERM objectives can often be optimized approximately using gradient-based methods (Bottou et al., 2018), while other hypothesis classes admit specialized optimization procedures. The ERM-oracle model abstracts away these implementations and measures the number of

optimization queries required for online prediction. We call a learner *oracle-efficient* if it makes at most polynomially many oracle queries in the horizon $T$.

Perhaps surprisingly, ERM oracles already suffice for *agnostic* transductive online learning, where the labels need not agree with any hypothesis. The random-playout algorithm of Cesa-Bianchi and Shamir (2011) (see also Cesa-Bianchi and Shamir, 2013; Rakhlin et al., 2012) achieves $O(\sqrt{T \log N})$ expected *regret*, measured against the best fixed hypothesis in $\mathcal{H}$, using only two ERM queries per round. In the realizable setting, the best hypothesis makes no mistakes, so the same algorithm guarantees $O(\sqrt{T \log N})$ *expected mistakes*. Thus, polynomially many ERM queries suffice for sublinear mistakes whenever $\log N = o(T)$.

This leads to our central question: *Can realizability improve the mistake bound of an oracle-efficient transductive learner beyond the agnostic rate?* In particular, can polynomially many ERM calls recover the logarithmic bound of halving? We show that, for general finite hypothesis classes, the aforementioned square-root rate *cannot* be improved in the worst case.

**The ERM oracle.** For any weight vector $w \in \mathbb{R}^T$, the oracle returns the full maximizing trace

$$\mathsf{ERM}_{\mathcal{H}}(w) := \operatorname{lexmin}\left(\arg\max_{h \in \mathcal{H}} w \cdot h\right), \tag{1}$$

where $w \cdot h = \sum_{t=1}^{T} w_t h_t$ and lexmin selects the lexicographically smallest maximizer. This oracle subsumes weighted ERM for any binary prediction loss $\ell : \{0,1\} \times \{0,1\} \to \mathbb{R}$. Indeed, given labels $y_1, \ldots, y_T \in \{0,1\}$ and nonnegative weights $a_1, \ldots, a_T$, let $w_t = a_t\big(\ell(0, y_t) - \ell(1, y_t)\big)$. Then

$$\sum_{t=1}^{T} a_t \ell(h_t, y_t) = \sum_{t=1}^{T} a_t \ell(0, y_t) - w \cdot h, \tag{2}$$

so a single oracle call returns a minimizer of the weighted empirical loss.

Our oracle is deliberately strong: it accepts arbitrary real-valued weights and reveals the entire optimizing trace. It can therefore simulate weaker oracle forms that restrict the admissible weights or reveal only part of the optimizer, provided they use the same tie-breaking rule. The learner may randomize, issue adaptive queries before and during prediction, and perform *unlimited computation* between oracle calls. Its only access to the hypothesis class $\mathcal{H}$ is through the oracle.

**The main result.** Write $M_T = \sum_{t=1}^{T} \mathbf{1}\{\widehat{y}_t \neq h_t^\star\}$ for the learner's number of mistakes. Throughout, log means $\log_2$ and ln means the natural logarithm.

**Theorem 1.1** (Polynomial-query lower bound)**.** *Fix $\beta \in (0,1)$. There is a constant $c_\beta > 0$ such that for every fixed $C > 0$ and all sufficiently large $T$, with $N = 2^{\lfloor T^\beta \rfloor}$, the following holds. For every randomized transductive learner $\mathcal{A}$ using at most $T^C$ queries to (1) on every execution, there are a fixed class $\mathcal{H} \subseteq \{0,1\}^T$ of exactly $N$ distinct traces and a fixed $h^\star \in \mathcal{H}$ for which*

$$\mathbb{E}_{\mathcal{A}} M_T \;\geq\; c_\beta \sqrt{T \log N}. \tag{3}$$

*The pair $(\mathcal{H}, h^\star)$ may depend on $\mathcal{A}$; $c_\beta$ does not depend on $C$.*

The random-playout upper bound discussed above matches Theorem 1.1 up to constant factors, establishing that for $N = 2^{\lfloor T^\beta \rfloor}$, the optimal worst-case expected mistake bound among learners making polynomially many oracle queries is $\Theta_\beta(\sqrt{T \log N})$, in sharp contrast to the $O(\log N)$ bound from halving. The separation persists even for much smaller classes: Theorem 8.1 establishes a lower bound of $\exp(\Omega(\log T / \log\log T))$ mistakes when $\log N = \Theta((\log T)^2)$, whereas halving makes only $O((\log T)^2)$ mistakes.

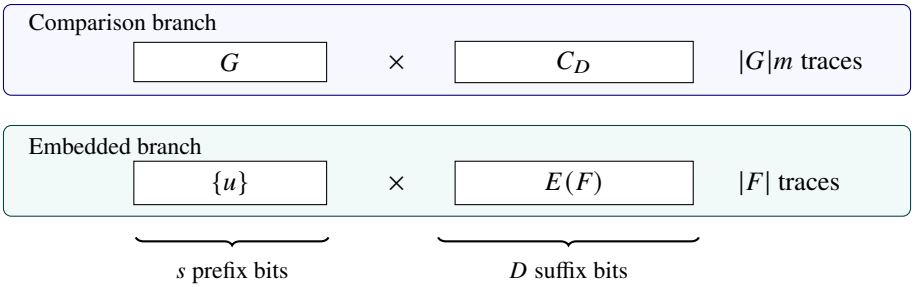



Figure 1: Composition of two realizable class–label pairs. The comparison branch contains $G \times C_D$. The embedded branch contains the fresh class $E(F)$ only after the realized prefix $u$. The label sequence $u\|E(v)$ belongs to the embedded branch.

**How the proof works.** We prove the lower bound by constructing a distribution over realizable pairs $(\mathcal{H}, h^\star)$; the learner knows the distribution but not its realization. The construction combines two independently drawn pairs $(G, u)$ and $(F, v)$, where $G \subseteq \{0,1\}^s$, $u \in G$, $F \subseteq \{0,1\}^r$, and $v \in F$. The first pair describes the labels in the first $s$ rounds, and the second describes the labels to be predicted after. We randomly embed the $r$ coordinates of $F$ into $D = Br$ new coordinates by an injective map $E$, and choose a fixed set $C_D \subseteq \{0,1\}^D$ of $m$ comparison traces. The resulting class and realizable label sequence are

$$\mathcal{H} = (G \times C_D) \cup (\{u\} \times E(F)), \qquad h^\star = u\|E(v), \tag{4}$$

where $\|$ denotes concatenation. The first branch consists of all prefix traces in $G$ paired with traces in $C_D$. The second consists of the embedded class $E(F)$, with the *same* realized prefix $u \in G$. Consequently,

$$|\mathcal{H}| \le |G|\, m + |F|.$$

Our main goal is to show that the combined problem $(\mathcal{H}, h^\star)$ retains the difficulty of both problems $(G, u)$ and $(F, v)$. We show that $C_D$ can be chosen so that any ERM query returning a trace from $\{u\} \times E(F)$ must induce a halfspace of small uniform measure. A Fourier estimate and Boolean hypercontractivity then show that, for any fixed query, this event occurs with probability at most $\alpha$ over the random embedding $E$ (Lemmas 3.1 to 4.2). The bound extends to adaptive queries by comparing the actual learner with one whose oracle uses only the first branch. Until their oracle outputs first differ, both learners receive identical information and make identical queries, independently of $E$. Consequently, the first $s$ rounds retain an expected mistake lower bound of $b_L - sQ\alpha$, where $b_L$ is the lower bound for the first prediction problem $(G, u)$ and $Q$ is the number of oracle queries.

For the last $D$ rounds, a learner given the realized prefix $u$ and the embedding $E$ can simulate each ERM query to the combined class using at most one query to $F$. Thus, these rounds retain an expected mistake lower bound of $b_R$, where $b_R$ is the lower bound for the second prediction problem $(F, v)$, without increasing the query budget. Combining the two bounds, the composition lemma yields

$$\mathbb{E}M_{s+D} \ge b_L + b_R - sQ\alpha, \qquad \alpha = \sqrt{2}(D+1)n^{1/(B+1)}m^{-1/2}, \tag{5}$$

where $n = |F|$. By choosing $m$ sufficiently large, the error $sQ\alpha$ can be made negligible for polynomial $Q$.

Iterating the composition lemma allows mistake lower bounds to accumulate while keeping the logarithm of the class size small. For example, starting with Boolean cubes of dimension $B^2$ under uniformly random labels, a single level of composition combining $B$ copies yields a problem with horizon $T = \Theta(B^4)$, logarithmic class size $\log N = \Theta(B^2)$, and expected mistake lower bound $\Omega(B^3) = \Omega(\sqrt{T \log N})$. Further levels of composition establish the full range of exponents in Theorem 1.1 and extend the separation to much smaller hypothesis classes in Theorem 8.1.

**Related work.** Transductive online learning was studied by Ben-David et al. (1997); Kakade and Kalai (2005), and random playout achieves the agnostic-rate upper bound (Cesa-Bianchi and Shamir, 2013). The closest lower bounds are due to Attias et al. (2025): their ERM lower bound applies to deterministic learners making fewer than $T/2$ queries, while their randomized lower bound allows at most $T/20$ queries to a weaker consistency oracle. Our result strengthens both bounds, applying to randomized learners making *any fixed polynomial* number of queries, even with access to a weighted-ERM oracle that accepts arbitrary real linear objectives and returns a complete maximizing hypothesis. In the regime of Theorem 1.1, our lower bound matches the agnostic-rate upper bound, establishing that polynomially many ERM queries *cannot* recover the logarithmic mistake bound of halving. This settles the polynomial-query question, while exponentially large query budgets fall outside our scope. Further comparisons appear in Section 9.

**Organization.** We formalize the distributional model in Section 2, prove the hiding and composition lemmas in Sections 3 to 5, and establish the main and small-class bounds in Sections 6 to 8.

## 2 Model and distributional lower bounds

**Protocol.** Fix a horizon $T \geq 1$. A finite nonempty class $\mathcal{H} \subseteq \{0,1\}^T$ and a target $h^\star \in \mathcal{H}$ are fixed before the interaction begins; the learner knows $T$ but does not receive $\mathcal{H}$. In each round $t = 1, \ldots, T$, the learner may issue oracle queries, chosen adaptively on the basis of its internal randomness, the labels $h^\star_1, \ldots, h^\star_{t-1}$, and all previous oracle answers; it then predicts $\widehat{y}_t \in \{0,1\}$ and observes $h^\star_t$. A query $w \in \mathbb{R}^T$ is answered with the full trace $\mathsf{ERM}_{\mathcal{H}}(w)$ defined in (1); no other access to $\mathcal{H}$ is available. The number of mistakes is

$$M_T = \sum_{t=1}^{T} \mathbf{1}\{\widehat{y}_t \neq h^\star_t\}.$$

Queries made before round 1 are permitted and count toward the budget. A learner is a *$Q$-query learner* if it makes at most $Q$ oracle calls on every possible transcript, including those inconsistent with the hypothesis class. This requirement is without loss of generality: any learner satisfying the query bound on realizable transcripts can be truncated after $Q$ calls without changing its behavior on the consistent transcripts. We impose this convention because the proof of Lemma 5.2 simulates oracle answers from a class different from the realized one. Learners may be randomized, make predictions outside $\mathcal{H}$, and perform unlimited computation, including exact real arithmetic, between oracle calls.

**Distributional lower bounds.** We establish lower bounds using distributions $\mathscr{D}$ over pairs $(\mathcal{H}, h^\star)$, where $h^\star \in \mathcal{H}$ almost surely. Define

$$L_Q(\mathscr{D}) := \inf_{\mathcal{A}} \mathbb{E}_{(\mathcal{H},h^\star)\sim\mathscr{D},\,\mathcal{A}}[M_T], \tag{6}$$

where the infimum ranges over all $Q$-query learners $\mathcal{A}$. We allow the learner to know the distribution $\mathscr{D}$, the horizon and class size, all public parameters of the construction, and the oracle's tie-breaking rule. Only the realized class $\mathcal{H}$ and target $h^\star$ are hidden. Thus, our lower bounds hold even when the learner knows exactly how the hard instances are generated.

**From distributions to fixed instances.** For technical convenience, our construction first samples a target prefix and then uses it to define part of the hypothesis class. Nevertheless, the entire pair $(\mathcal{H}, h^\star)$ is sampled before prediction begins; neither the class nor the target changes during learning. Equivalently, one may first sample $\mathcal{H}$ from its marginal distribution and then $h^\star$ from the corresponding conditional distribution. If

$L_Q(\mathscr{D}) \geq L$, then, by averaging, for every $Q$-query learner $\mathcal{A}$, there *exists* a fixed pair $(\mathcal{H}, h^\star)$ in the support of $\mathscr{D}$ such that

$$\mathbb{E}_{\mathcal{A}}[M_T] \geq L.$$

Thus, our distributional lower bounds imply worst-case lower bounds for fixed realizable instances.

**The tie-breaking rule.** We order binary words lexicographically with $0 < 1$: $x$ precedes $y$ if $x_k < y_k$ at their first differing coordinate. The oracle always returns the lexicographically smallest maximizer, using a fixed rule known to the learner. Specifying this rule is important because the learner can deliberately create ties, for example by querying $w = 0$. As shown in Section 5.1, lexicographic tie-breaking is equivalent to maximizing a sufficiently small, class-independent perturbation of the objective. Since a universal guarantee must hold for every valid implementation of weighted ERM, our lower bound for this particular implementation rules out such guarantees. We do not claim that the lower bound holds for arbitrary class-dependent tie-breaking rules, which could reveal additional information through the choice of maximizer. Indeed, Li (2026) shows that tie-breaking can affect the oracle complexity of consistency-type oracles.

## 3 Optimizer density under a random embedding

**The random embedding.** Fix a nonempty class $F \subseteq \{0,1\}^r$ with $|F| \leq n$ and an odd integer $B \geq 3$, and let $D = Br$. The oddness assumption is needed only for the elementary proof of hypercontractivity in Section A. We construct a random embedding $E : F \to \{0,1\}^D$ by choosing a uniformly random subset

$$S = \{i_1 < \cdots < i_r\} \subseteq [D]$$

of size $r$ and an independent uniform mask $X \in \{0,1\}^D$. For every $f \in F$, define

$$E(f) = X \oplus \iota_S(f), \qquad \iota_S(f)_{i_j} = f_j \ \ (j \in [r]), \qquad \iota_S(f)_i = 0 \ \ (i \notin S), \tag{7}$$

where $\oplus$ denotes coordinatewise XOR. The same support $S$ and mask $X$ are used for all $f \in F$. Thus, $E$ is injective, and each fixed $E(f)$ is uniformly distributed over $\{0,1\}^D$, although the embedded traces are correlated. For $x \in \{0,1\}^D$, we write $x_S = (x_{i_1}, \ldots, x_{i_r})$ for its restriction to the coordinates in $S$.

Fix an objective $w \in \mathbb{R}^D$ independently of $(S, X)$, and let

$$Y := \operatorname{lexmin}\Big(\arg\max_{y \in E(F)} w \cdot y\Big)$$

be the oracle's output on the embedded class. Although each individual $E(f)$ is uniformly distributed over $\{0,1\}^D$, the maximizer $Y$ need not be uniform, since the optimization selects among correlated embedded traces. The following lemma controls this selection bias uniformly over all fixed objectives $w$.

**Lemma 3.1** (Density bound for the optimizer)**.** *Let $\mu_D$ be the uniform probability measure on $\{0,1\}^D$. For every set $A \subseteq \{0,1\}^D$ and every fixed $w \in \mathbb{R}^D$,*

$$\mathbb{P}_{S,X}(Y \in A) \ \leq \ n^{1/(B+1)} \sqrt{\mu_D(A)}. \tag{8}$$

*The bound holds for every fixed $F$ with $|F| \leq n$.*

*Proof.* All Boolean cubes are equipped with the uniform measure, and we write $\|a\|_p = (\mathbb{E}|a|^p)^{1/p}$. The proof has four steps.

*Step 1: Bound the density conditional on the support.* Fix $S$. Since all candidates in $E(F)$ agree with $X$ outside $S$, their weighted scores differ only on $S$. Thus, for fixed $S$, $w$, and $F$, the optimizer $Y_S$ depends only on $X_S$, while $Y_{S^c} = X_{S^c}$ remains independent and uniform. Let

$$\varphi_S(z) = 2^r \mathbb{P}(Y_S = z \mid S)$$

be the density of $Y_S$ relative to the uniform measure on $\{0,1\}^r$. Since $Y_S = X_S \oplus f$ for some $f \in F$,

$$\{Y_S = z\} \subseteq \bigcup_{f \in F} \{X_S = z \oplus f\}.$$

Each event in the union has probability $2^{-r}$, so

$$0 \le \varphi_S(z) \le |F| \le n, \qquad \mathbb{E}_z \varphi_S(z) = 1. \tag{9}$$

Let $\psi$ denote the density of $Y$ relative to the uniform measure $\mu_D$ on $\{0,1\}^D$. Conditional on $S$, the coordinates $Y_{S^c}$ are uniformly distributed over $\{0,1\}^{S^c}$ and independent of $Y_S$. Thus, the conditional density of $Y$ with respect to $\mu_D$ is $\varphi_S(x_S)$. Averaging over $S$ gives

$$\psi(x) = \mathbb{E}_S \varphi_S(x_S). \tag{10}$$

For any $A \subseteq \{0,1\}^D$, Cauchy–Schwarz gives

$$\mathbb{P}(Y \in A) = \mathbb{E}_{x \sim \mu_D}[\psi(x) \mathbf{1}_A(x)] \le \|\psi\|_2 \sqrt{\mu_D(A)}.$$

It therefore suffices to prove $\|\psi\|_2 \le n^{1/(B+1)}$.

*Step 2: Reduce to the intersection of two supports.* Let $S, S'$ be independent uniform $r$-subsets of $[D]$, and write $I = S \cap S'$. Expanding (10),

$$\|\psi\|_2^2 = \mathbb{E}_{S,S'} \mathbb{E}_x[\varphi_S(x_S)\varphi_{S'}(x_{S'})]. \tag{11}$$

Conditional on $x_I$, the two factors $x_S$ and $x_{S'}$ depend on disjoint sets of remaining coordinates and are therefore independent. Writing

$$a_I = \mathbb{E}[\varphi_S(x_S) \mid x_I], \qquad b_I = \mathbb{E}[\varphi_{S'}(x_{S'}) \mid x_I],$$

the inner expectation in (11) equals $\mathbb{E}[a_I b_I]$. Using $2a_I b_I \le a_I^2 + b_I^2$ and the symmetry between $S$ and $S'$ yields

$$\|\psi\|_2^2 \le \mathbb{E}_{S,S'} \big\| \mathbb{E}[\varphi_S(x_S) \mid x_I] \big\|_2^2. \tag{12}$$

*Step 3: Bound the contribution at each Fourier degree.* For $U \subseteq [D]$, let $\chi_U(x) = (-1)^{\sum_{i \in U} x_i}$. Viewing $\varphi_S(x_S)$ as a function on $\{0,1\}^D$, its Fourier expansion is

$$\varphi_S(x_S) = \sum_{U \subseteq S} \widehat{\varphi}_S(U) \chi_U(x), \qquad \widehat{\varphi}_S(U) = \mathbb{E}_x[\varphi_S(x_S)\chi_U(x)].$$

Conditioning on $x_I$ keeps only the characters indexed by subsets of $I$. Hence, Parseval's identity gives

$$\big\| \mathbb{E}[\varphi_S(x_S) \mid x_I] \big\|_2^2 = \sum_{U \subseteq I} \widehat{\varphi}_S(U)^2.$$

For $U \subseteq S$, the condition $U \subseteq I$ is equivalent to $U \subseteq S'$. Averaging over $S'$ in (12), we obtain

$$\|\psi\|_2^2 \le \mathbb{E}_S \sum_{U \subseteq S} \widehat{\varphi}_S(U)^2 \mathbb{P}(U \subseteq S') \le \mathbb{E}_S \sum_{U \subseteq S} B^{-|U|} \widehat{\varphi}_S(U)^2. \tag{13}$$

The last inequality follows because, for $|U| = k \le r$,

$$\mathbb{P}(U \subseteq S') = \frac{\binom{D-k}{r-k}}{\binom{D}{r}} = \prod_{i=0}^{k-1} \frac{r-i}{D-i} \le \left(\frac{r}{D}\right)^k = B^{-k}. \tag{14}$$

*Step 4: Apply hypercontractivity.* Let $\mathrm{T}_\rho$ denote the Boolean noise operator, defined so that $\mathrm{T}_\rho\varphi$ has Fourier coefficients $\widehat{\mathrm{T}_\rho\varphi}(U) = \rho^{|U|}\widehat{\varphi}(U)$. By Parseval's identity, (13) becomes

$$\|\psi\|_2^2 \le \mathbb{E}_S \|\mathrm{T}_{1/\sqrt{B}}\varphi_S\|_2^2.$$

The $(p, 2)$-hypercontractive inequality (Bonami, 1970), see also O'Donnell (2014, Chapter 9), states that $\|\mathrm{T}_\rho\varphi\|_2 \le \|\varphi\|_p$ whenever $1 \le p \le 2$ and $0 \le \rho \le \sqrt{p-1}$. Taking $p = 1 + 1/B$ and $\rho = 1/\sqrt{B}$ gives

$$\|\mathrm{T}_{1/\sqrt{B}}\varphi\|_2 \le \|\varphi\|_{1+1/B}. \tag{15}$$

A self-contained proof for odd $B$ is given in Section A.

Finally, (9) implies

$$\|\varphi_S\|_p^p = \mathbb{E}\varphi_S^p \le n^{p-1}\mathbb{E}\varphi_S = n^{1/B},$$

and therefore

$$\|\varphi_S\|_p \le n^{1/(B+1)}.$$

Combining this with (13) and (15) yields $\|\psi\|_2^2 \le n^{2/(B+1)}$. The bound (8) now follows from Step 1. □

# 4 Comparison sets for linear queries

Let $C_D \subseteq \{0,1\}^D$ be a fixed set of comparison traces. For a linear query, an optimizer over the embedded class $E(F)$ can outperform every element of $C_D$ only if it lies in a halfspace disjoint from $C_D$. We therefore construct $C_D$ to intersect every halfspace of sufficiently large uniform measure. The existence of such a set follows from a probabilistic argument using the Sauer–Shelah lemma (Sauer, 1972), since affine halfspaces in $\mathbb{R}^D$ have VC dimension at most $D + 1$.

**Lemma 4.1** (A public comparison set)**.** *For every integer $1 \le m \le 2^D$ there is a set $C_D \subseteq \{0,1\}^D$ of exactly $m$ traces that intersects every strict affine halfspace $A = \{x \in \{0,1\}^D : w \cdot x > a\}$, with $w \in \mathbb{R}^D$ and $a \in \mathbb{R}$, for which*

$$\mu_D(A) > \varepsilon_D, \qquad \varepsilon_D := \frac{2(D+1)^2}{m}. \tag{16}$$

*Proof.* If $\varepsilon_D \ge 1$, the claim is immediate, since every subset of $\{0,1\}^D$ has uniform measure at most 1. Otherwise, sample $m$ distinct points uniformly without replacement from $\{0,1\}^D$. A fixed set $A \subseteq \{0,1\}^D$ is missed with probability

$$\binom{2^D - |A|}{m} \Big/ \binom{2^D}{m} \le (1 - \mu_D(A))^m \le e^{-m\mu_D(A)}.$$

To apply a union bound over all halfspaces, we first bound the number of distinct subsets they induce on $\{0,1\}^D$. Since strict affine halfspaces in $\mathbb{R}^D$ have VC dimension at most $D + 1$, the Sauer–Shelah lemma (Sauer, 1972) implies that the number of distinct intersections with $\{0,1\}^D$ is at most

$$\sum_{k=0}^{D+1} \binom{2^D}{k} \le (2^D + 1)^{D+1}.$$

Consequently, by a union bound, the probability that the sampled set misses some halfspace of uniform measure greater than $\varepsilon_D$ is at most

$$(2^D+1)^{D+1}e^{-m\varepsilon_D} = (2^D+1)^{D+1}e^{-2(D+1)^2} < 1,$$

where the last inequality follows from $\ln(2^D+1) < 2(D+1)$. Therefore, there exists a fixed set $C_D$ of size $m$ intersecting every halfspace of uniform measure greater than $\varepsilon_D$. □

**Lemma 4.2** (Probability of outperforming the comparison set)**.** *Let $E$ be the random embedding of Section 3, with $|F| \le n$, and let $C_D$ be as in Lemma 4.1. For every fixed $w \in \mathbb{R}^D$ chosen independently of the embedding,*

$$\mathbb{P}\Big(\max_{f\in F} w\cdot E(f) > \max_{c\in C_D} w\cdot c\Big) \;\le\; \alpha(n,D,m) := \sqrt{2}\,(D+1)\,n^{1/(B+1)}\,m^{-1/2}. \tag{17}$$

*Here $\alpha$ also depends on the expansion factor $B = D/r$, which we suppress from the notation.*

*Proof.* Let $b_w = \max_{c\in C_D} w\cdot c$ and $A_w = \{x \in \{0,1\}^D : w\cdot x > b_w\}$. Since $A_w$ is disjoint from $C_D$, Lemma 4.1 gives $\mu_D(A_w) \le \varepsilon_D$. Let $Y$ be the optimizer over $E(F)$. The event in (17) is precisely $\{Y \in A_w\}$. By Lemma 3.1 and (16), its probability is at most $n^{1/(B+1)}\sqrt{\varepsilon_D} = \alpha_B(n,D,m)$. □

Writing $g = \log n$ and $a = \log m$, the bound is

$$\alpha(n,D,m) = \sqrt{2}\,(D+1)\,2^{g/(B+1)-a/2}. \tag{18}$$

In particular, $a \ge 4g/B$ implies $\alpha(n,D,m) \le \sqrt{2}(D+1)2^{-g/B}$. The parameter choices in Section 6 make this smaller than every fixed inverse polynomial in the final horizon.

# 5 Adaptive composition

Lemma 4.2 controls a *fixed* query. On its own it does not handle an adaptive learner, whose later queries may depend on earlier oracle answers. To handle adaptivity, we compare the actual execution with a reference execution whose oracle is restricted to the first branch. We also show that predicting the last $D$ labels remains at least as hard as the original prediction problem on $F$. Together, these two arguments establish that the mistake lower bounds of both components are preserved under composition.

## 5.1 Lexicographic tie-breaking

Tie-breaking creates two difficulties in the reductions. First, the full oracle and the comparison-only oracle may return different maximizers with equal scores, so their disagreement need not satisfy the strict inequality in Lemma 4.2. Second, XOR masking does not preserve lexicographic order, so the inner oracle may break ties differently from the outer oracle. We resolve both issues by implementing lexicographic tie-breaking through a sufficiently small, class-independent perturbation of the objective in the full outer dimension.

**Lemma 5.1** (Class-independent lexicographic perturbation)**.** *For every dimension $L$ and every $w \in \mathbb{R}^L$ there is $\delta > 0$, depending only on $(L, w)$, such that the refined objective*

$$\widetilde{w}_i = w_i - \delta 2^{-i}, \qquad i \in [L], \tag{19}$$

*assigns distinct scores to distinct words of $\{0,1\}^L$. In particular, for every nonempty $K \subseteq \{0,1\}^L$, the objective $\widetilde{w}$ has a unique maximizer over $K$, and this maximizer is $\mathsf{ERM}_K(w)$.*

*Proof.* Let $\kappa(x) = \sum_{i=1}^{L} 2^{-i} x_i$. If $x \neq y$ first differ at coordinate $k$, then $\kappa(x) - \kappa(y)$ has the sign of $x_k - y_k$, because $2^{-k} > \sum_{i=k+1}^{L} 2^{-i}$. Thus $\kappa$ strictly represents the lexicographic order, and $|\kappa(x) - \kappa(y)| < 1$ for all $x, y$. If not all words have the same $w$-score, let $\gamma > 0$ be the minimum of $|w \cdot x - w \cdot y|$ over pairs with different scores (it exists because the cube is finite) and set $\delta := \gamma/2$; otherwise set $\delta := 1$. Since $\widetilde{w} \cdot x = w \cdot x - \delta\kappa(x)$, the perturbation preserves every strict comparison of $w$-scores and breaks every tie in favor of the lexicographically smaller word. Hence distinct words have distinct refined scores, and the unique $\widetilde{w}$-maximizer over $K$ is the lexicographically smallest $w$-maximizer. □

The refinement is an analytical device: the learner still asks $w$, but a simulator may compute the unique maximizer under $\widetilde{w}$, which is exactly the oracle's answer to $w$. Since $\delta$ is determined by the whole cube rather than by the unknown class, computing it requires no information about the class. In the suffix reduction below it is essential to refine first, in the full dimension, and only then restrict to the masked support.

## 5.2 The additive composition lemma

Let $\mathscr{D}_L$ and $\mathscr{D}_R$ be distributions over pairs $(G, u)$ and $(F, v)$ with $G \subseteq \{0,1\}^s$ and $F \subseteq \{0,1\}^r$, and suppose that $|F| \leq n$ almost surely. Fix an odd $B \geq 3$, set $D = Br$, and fix a public $m$-trace comparison set $C_D$ given by Lemma 4.1; $B$ and $m$ are fixed throughout this section. Draw $(G, u) \sim \mathscr{D}_L$, $(F, v) \sim \mathscr{D}_R$ and the embedding $(S, X)$ of (7) mutually independently. The *composed distribution* $\mathscr{D}_L \star \mathscr{D}_R$ is the law of

$$\mathcal{H} = (G \times C_D) \cup \big(\{u\} \times E(F)\big), \qquad h^\star = u \| E(v). \tag{20}$$

It has horizon $s + D$, it is always realizable, and $|\mathcal{H}| \leq |G|m + n$.

**Lemma 5.2** (Additive composition)**.** *Let $Q \geq 1$. If $L_Q(\mathscr{D}_L) \geq b_L$ and $L_Q(\mathscr{D}_R) \geq b_R$, then*

$$L_Q(\mathscr{D}_L \star \mathscr{D}_R) \;\geq\; b_L + b_R - sQ\,\alpha(n, D, m). \tag{21}$$

*Proof.* Fix a $Q$-query learner $\mathcal{A}$ for the composed prediction problem, and write $M_{\text{prefix}}$ and $M_{\text{suffix}}$ for its numbers of mistakes in rounds $1, \ldots, s$ (the *prefix*) and $s+1, \ldots, s+D$ (the *suffix*). We bound their expectations separately.

*Part I: a reference execution.* Consider the *reference execution* of $\mathcal{A}$, in which the prefix labels are the true labels $u_1, \ldots, u_s$ but every oracle query is answered from the comparison branch $G \times C_D$ instead of the full class $\mathcal{H}$. A learner $\mathcal{A}_L$ for the problem $\mathscr{D}_L$ can simulate the prefix of this execution with one query to $\mathsf{ERM}_G$ per outer query. Indeed, for $w = (w_L, w_R)$ with $w_L \in \mathbb{R}^s$ and $w_R \in \mathbb{R}^D$,

$$\max_{(x,c) \in G \times C_D} w \cdot (x, c) = \max_{x \in G} w_L \cdot x + \max_{c \in C_D} w_R \cdot c, \tag{22}$$

and the lexicographically smallest maximizer over the product is the concatenation of the lexicographically smallest maximizers over the two factors. Since $C_D$ is public, the second factor requires no oracle calls, and $\mathcal{A}_L$ uses each left label only after it is revealed. Because the query bound holds on every transcript (Section 2), $\mathcal{A}_L$ makes at most $Q$ queries even though the comparison-only query outputs need not come from the realized class. Thus $\mathcal{A}_L$ is a $Q$-query learner for $\mathscr{D}_L$ whose mistakes are exactly the reference execution's prefix mistakes, and

$$\mathbb{E}\big[M^{\text{ref}}_{\text{prefix}}\big] \;\geq\; b_L. \tag{23}$$

*Part II: coupling the adaptive executions.* Call a query a *prefix query* if it is issued before the prediction $\widehat{y}_s$; only prefix queries can influence prefix predictions. Run the reference and actual executions with the same random tape; both see the same prefix labels $u$. Condition on $(G, u)$, on the tape, and on $(F, v)$. Then the reference execution's prefix queries $w^{(1)}, \ldots, w^{(K)}$, $K \leq Q$, are fixed—including queries chosen adaptively

after earlier prefix labels—while $(S, X)$ remains uniformly distributed and independent of them. Let $\mathcal{L}_i$ be the event that the full oracle's output to $w^{(i)}$ differs from the comparison-only output.

Fix $i$, and let $\widetilde{w}$ be the refinement of $w = w^{(i)}$ from Lemma 5.1 in dimension $s + D$. On $\mathcal{L}_i$, the unique $\widetilde{w}$-maximizer over $\mathcal{H}$ does not belong to the comparison branch; hence it equals $(u, E(f))$ for some $f \in F$, and it strictly beats every comparison-branch trace under $\widetilde{w}$. Since $(u, c)$ is a comparison-branch trace for every $c \in C_D$,

$$\begin{aligned} \widetilde{w} \cdot (u, E(f)) &> \widetilde{w} \cdot (u, c) \qquad \text{for all } c \in C_D, \\ \text{and hence} \qquad \widetilde{w}_R \cdot E(f) &> \max_{c \in C_D} \widetilde{w}_R \cdot c. \end{aligned} \tag{24}$$

The suffix objective $\widetilde{w}_R$ is determined by $w^{(i)}$, not by the embedding, so Lemma 4.2 applied to $\widetilde{w}_R$ gives

$$\mathbb{P}(\mathcal{L}_i \mid G, u, \text{tape}, F, v) \le \alpha(n, D, m).$$

If the actual and reference prefix transcripts differ, consider the first prefix query at which their outputs differ. All earlier outputs and labels agree, so this query is $w^{(i)}$ for some $i$, and $\mathcal{L}_i$ occurs. (We never apply the fixed-query bound conditionally on a history that contains query outputs from the embedded branch.) By a union bound over $i \le K \le Q$,

$$\mathbb{P}(\text{some prefix query output differs}) \;\le\; Q\,\alpha(n, D, m). \tag{25}$$

Without a disagreement, the two executions make identical prefix predictions; with one, their prefix mistake counts differ by at most $s$. By (23) and (25),

$$\mathbb{E}\big[M^{\text{act}}_{\text{prefix}}\big] \;\ge\; b_L - sQ\,\alpha(n, D, m). \tag{26}$$

*Part III: simulate the composed learner using the right oracle.* For the suffix, we use a separate reduction: a learner $\mathcal{A}_R$ for the problem $\mathscr{D}_R$ that simulates the *actual* composed execution. The learner $\mathcal{A}_R$ samples $(G, u) \sim \mathscr{D}_L$ and $(S, X)$ itself, so it knows them completely, and it knows the public set $C_D$; it accesses $F$ only through $\mathsf{ERM}_F$ and the sequentially revealed labels of $v$.

*Oracle outputs.* Given an outer query $w = (w_L, w_R)$, the learner $\mathcal{A}_R$ refines the full objective to $\widetilde{w}$ (Lemma 5.1) and computes the maximizer over $G \times C_D$ locally. For a hypothesis in the embedded branch, the bit identity $b \oplus x = x + (1 - 2x)b$ yields

$$\widetilde{w} \cdot (u, E(f)) = \widetilde{w}_L \cdot u + \widetilde{w}_R \cdot X + \sum_{j=1}^{r} (1 - 2X_{i_j})\, \widetilde{w}_{R,i_j}\, f_j, \tag{27}$$

where $\widetilde{w}_{R,i}$ denotes the coefficient of suffix coordinate $i$ in the refined $(s + D)$-dimensional objective. The learner $\mathcal{A}_R$ issues the single query

$$\lambda_j = (1 - 2X_{i_j})\, \widetilde{w}_{R,i_j}, \qquad j \in [r], \tag{28}$$

to $\mathsf{ERM}_F$. By (27), $\lambda \cdot f$ differs from the refined score of $(u, E(f))$ by a constant that does not depend on $f$. Since $E$ is injective and distinct words have distinct refined scores (Lemma 5.1), the map $f \mapsto \lambda \cdot f$ is injective on $F$, so the maximizer of $\lambda \cdot f$ over $F$ is unique and the inner oracle's tie-breaking rule is never invoked—even though the XOR mask may reverse lexicographic order. Finally, $\mathcal{A}_R$ returns whichever of the best trace in the comparison branch and the best trace in the embedded branch has the larger refined score. Equal scores can occur only when the two traces coincide. This reproduces the outer oracle's answer exactly, using exactly one inner call.

*Labels and predictions.* The learner $\mathcal{A}_R$ knows every prefix label (the prefix target is $u$) and every suffix label off the support (the suffix label at $i \notin S$ is $X_i$). At support coordinate $i_j$ the suffix label is $X_{i_j} \oplus v_j$. When the simulated learner predicts $\widehat{y}_{s+i_j}$, the learner $\mathcal{A}_R$ predicts $\widehat{v}_j = \widehat{y}_{s+i_j} \oplus X_{i_j}$, observes $v_j$, and feeds back $v_j \oplus X_{i_j}$ as the outer label. The mistake indicators coincide:

$$\mathbf{1}\{\widehat{v}_j \neq v_j\} = \mathbf{1}\{\widehat{y}_{s+i_j} \neq v_j \oplus X_{i_j}\}. \tag{29}$$

Because $i_1 < \cdots < i_r$, the learner $\mathcal{A}_R$ never needs $v_j$ before making its own $j$th prediction. All of its oracle calls, including those that simulate outer queries during the prefix, are made to $\mathsf{ERM}_F$, so $\mathcal{A}_R$ is a $Q$-query learner for $\mathscr{D}_R$. Its simulated execution has exactly the law of the actual composed execution, and its mistakes are the actual execution's mistakes at the $r$ support coordinates of the suffix. Hence

$$\mathbb{E}\big[M^{\mathrm{act}}_{\mathrm{suffix}}\big] \;\geq\; b_R. \tag{30}$$

Adding (26) and (30) proves (21). □

*Remark* 5.3 (The role of the tie-breaking rule). The proof uses the same known lexicographic rule for every version of the oracle. The refinement of Lemma 5.1 turns a changed answer into a *strict* improvement and, independently, makes the masked-suffix simulation exact. Assuming that ties occur with probability zero would be incorrect: the learner can query the zero vector or create ties deliberately.

# 6 Recursive amplification: mistakes versus class size

We now iteratively apply the composition lemma to amplify the mistake lower bound while controlling the growth of the hypothesis class. We refer to each application as an *append*, since it places a new prediction problem after the existing one.

## 6.1 The recursive distributions

Fix a base dimension $d \geq 1$, a number of copies $q \geq 2$ per level, a depth $J \geq 1$, and an odd expansion factor $B \geq 3$, all integers. The base distribution $\mathscr{D}_0$ has the full cube $\{0,1\}^d$ as its class and a uniformly random target in that cube. Its horizon is $t_0 = d$. Since the hypothesis class is fixed, oracle answers provide no additional information about the target beyond the previously observed labels, even when queries are chosen adaptively. Each unrevealed target bit therefore remains an independent fair coin, so every learner makes exactly $d/2$ mistakes in expectation.

At level $j \in [J]$, suppose $\mathscr{D}_{j-1}$ has horizon $t_{j-1}$. Draw $q$ independent instances from this distribution. Start with the first and append the remaining $q-1$ one at a time using (20). Each append uses a fresh embedding into $Bt_{j-1}$ suffix coordinates and a fixed public comparison set of size $m_j = 2^{a_j}$, where $a_j$ is an integer satisfying $1 \leq a_j \leq Bt_{j-1}$. Write $\star_j$ for this composition of distributions, with independent factors. If $\mathscr{P}_{j,k}$ denotes the law after combining the first $k$ instances, then

$$\mathscr{P}_{j,1} = \mathscr{D}_{j-1}, \qquad \mathscr{P}_{j,k+1} = \mathscr{P}_{j,k} \star_j \mathscr{D}_{j-1} \quad (1 \leq k < q), \qquad \mathscr{D}_j = \mathscr{P}_{j,q}.$$

The same comparison set is used for all appends at level $j$.

Overlaps between the comparison and embedded branches can reduce the number of distinct traces. Write $n_j$ for the *nominal class size* at level $j$, obtained by counting the two branches separately at every append. Every class drawn from $\mathscr{D}_j$ has at most $n_j$ traces, with equality if there are no overlaps in its construction.

## 6.2 Three recurrences

**Horizon.** The first copy contributes $t_{j-1}$ coordinates, and each of the other $q-1$ copies is expanded to $Bt_{j-1}$ coordinates. Thus

$$t_0 = d, \qquad t_j = \big[1 + (q-1)B\big]\, t_{j-1}, \qquad t_J = d\,\big[1 + (q-1)B\big]^J. \tag{31}$$

Write $\tau := t_J$ for the horizon before we pad the construction to a prescribed $T$ in Section 7.

**Class size.** Suppose the accumulated class has nominal size $P$. Each append creates a comparison branch of nominal size $Pm_j$ and an embedded branch of nominal size $n_{j-1}$. Thus, the nominal class size evolves according to $P \mapsto Pm_j + n_{j-1}$. Starting from $P = n_{j-1}$ and applying this recurrence $q-1$ times gives

$$n_0 = 2^d, \qquad n_j = n_{j-1}\big(1 + m_j + \cdots + m_j^{q-1}\big). \tag{32}$$

Let $g_j = \log n_j$. Since $m_j = 2^{a_j} \geq 2$, we have $m_j^{q-1} \leq \sum_{k=0}^{q-1} m_j^k \leq 2m_j^{q-1}$, and hence

$$g_{j-1} + (q-1)a_j \;\leq\; g_j \;\leq\; g_{j-1} + (q-1)a_j + 1. \tag{33}$$

Thus, each level increases the logarithmic class size by approximately $(q-1)a_j$.

**Mistakes.** Each base instance contributes $d/2$ to the lower bound. Each append subtracts the error term of Lemma 5.2. The right factor at level $j$ is $\mathscr{D}_{j-1}$, with class size at most $n_{j-1}$, so the probability bound for a fixed query is

$$\alpha_j := \alpha_B(n_{j-1}, Bt_{j-1}, m_j) = \sqrt{2}\,(Bt_{j-1}+1)\,2^{g_{j-1}/(B+1)-a_j/2}. \tag{34}$$

The left factor $\mathscr{P}_{j,k}$ has horizon $t_{j-1}(1+(k-1)B) < t_j$. Applying Lemma 5.2 to each of the $q-1$ appends with the same query budget $Q$ gives

$$L_Q(\mathscr{D}_j) \;\geq\; q\,L_Q(\mathscr{D}_{j-1}) - (q-1)\,t_j Q\,\alpha_j.$$

Since $L_Q(\mathscr{D}_0) = d/2$, induction on $j$ gives

$$L_Q(\mathscr{D}_J) \;\geq\; \frac{dq^J}{2} - Q\sum_{j=1}^{J}(q-1)q^{J-j}t_j\alpha_j \;\geq\; \frac{dq^J}{2} - (q^J-1)\,\tau Q \max_{1\leq j\leq J}\alpha_j.$$

Since $q^J \leq \tau$ by (31), we obtain

$$L_Q(\mathscr{D}_J) \;\geq\; \frac{dq^J}{2} - \tau^2 Q \max_{1\leq j\leq J}\alpha_j. \tag{35}$$

Increasing $m_j$ improves the fixed-query bound in (34) and raises the class-size cost in (33). We balance these two effects in the parameter choices below.

## 6.3 Making all class sizes exact

The nominal class size may overcount hypotheses if the two branches overlap. We show that such overlaps are sufficiently unlikely to be eliminated by conditioning, without significantly weakening the mistake lower bound. Consider an append at level $j$, with right class $F$ and suffix dimension $D = Bt_{j-1}$. Since the two

branches share only the realized prefix $u$, an overlap occurs precisely when $C_D \cap E(F) \neq \varnothing$. Conditional on $F$, each $E(f)$ is uniform on $\{0,1\}^D$. A union bound therefore gives

$$\mathbb{P}\big(C_D \cap E(F) \neq \varnothing \;\big|\; F\big) \le m_j |F|\, 2^{-D} \le 2^{a_j + g_{j-1} - Bt_{j-1}}. \tag{36}$$

The full recursive construction contains $(q-1)\sum_{j=1}^{J} q^{J-j} = q^J - 1$ appends. Let $\mathcal{E}$ denote the event that no overlap occurs at any append. By another union bound,

$$\zeta := \mathbb{P}(\mathcal{E}^c) \le (q^J - 1) \max_{j \in [J]} 2^{a_j + g_{j-1} - Bt_{j-1}}. \tag{37}$$

On $\mathcal{E}$, the resulting class has exactly $n_J$ distinct traces.

We now show that conditioning on $\mathcal{E}$ preserves the lower bound up to a negligible error. Let $\tau = t_J$ denote the horizon of the final composed problem, and let $M_\tau$ be the total number of mistakes over its $\tau$ rounds. Fix any $Q$-query learner for the conditioned distribution, and run the same learner on the unconditioned distribution, with the same announced horizon and class size. Since the query cap holds on every transcript by Section 2, the lower bound (35) applies to this learner even on instances where overlaps occur. Moreover, since $0 \le M_\tau \le \tau$, for $\zeta < 1$,

$$\mathbb{E}[M_\tau \mid \mathcal{E}] \ge \frac{\mathbb{E}[M_\tau] - \tau\zeta}{1-\zeta} \ge \mathbb{E}[M_\tau] - \frac{\tau\zeta}{1-\zeta}. \tag{38}$$

The parameter choices below ensure $\zeta = o(1/\tau)$. Thus, conditioning on $\mathcal{E}$ guarantees exactly $n_J$ hypotheses while reducing the mistake lower bound by only $o(1)$. Importantly, this conditioning is performed only after establishing the lower bound for the unconditioned recursive distribution.

### 6.4 A worked one-level example

A single level already illustrates the result. Let $B \to \infty$ through odd integers, and take $J = 1$, $d = B^2$, $q = B$ and $a_1 = 4B$. We combine $B$ full cubes of dimension $B^2$ with independent random targets. The horizon is

$$\tau = B^2\big[1 + (B-1)B\big] = \Theta(B^4).$$

The nominal class size is

$$n_1 = 2^{B^2}\big(1 + 2^{4B} + \cdots + 2^{4B(B-1)}\big), \qquad \log n_1 = B^2 + 4B(B-1) + O(1) = \Theta(B^2).$$

The fixed-query bound is $\alpha_1 \le \sqrt{2}\,(B^3+1)2^{-B}$, and the overlap probability is at most $(B-1)2^{4B+B^2-B^3}$. Combining (35) and (38), every learner making polynomially many queries incurs at least $B^3/2 - o(1)$ expected mistakes under the distribution conditioned on no overlaps. Thus $\log n_1 = \Theta(\tau^{1/2})$ and the lower bound is $\Omega(\tau^{3/4}) = \Omega(\sqrt{\tau \log n_1})$. This proves Theorem 1.1 for $\beta = \frac{1}{2}$.

## 7 Matching the agnostic square-root rate

We now choose the recursion parameters to match the agnostic square-root rate. At each level, we set $q = B$. Meanwhile, we choose the comparison set sizes so that the logarithm of the class size remains $\Theta(d)$ across all levels. Starting from $d/2$ expected mistakes over $d$ rounds, these scalings yield a mistake lower bound of order $\sqrt{\tau d} = \Theta(\sqrt{\tau \log n_J})$.

### 7.1 Choosing the depth and comparison-set sizes

Fix $\beta \in (0,1)$, and set

$$J := \left\lfloor \frac{1-\beta}{2\beta} \right\rfloor + 1, \qquad \theta := \frac{1-\beta}{2\beta J} \in (0,1). \tag{39}$$

The argument works for any integer $J > (1-\beta)/(2\beta)$. As $d \to \infty$, let $B$ be the least odd integer at least $d^\theta$, so $B \sim d^\theta$, and set $q = B$. Choose the comparison-set exponent

$$a_j = \left\lceil \frac{4g_{j-1}}{B} \right\rceil. \tag{40}$$

Here $g_{j-1}$ is determined by the nominal class-size recurrence, so all comparison-set sizes are fixed before sampling any instances. To verify that they fit in their suffix cubes, first bound the nominal sizes. By (33) and (40),

$$g_j \;\le\; g_{j-1} + (B-1)\Big(\frac{4g_{j-1}}{B} + 1\Big) + 1 \;\le\; 5g_{j-1} + B.$$

Since $g_0 = d$, induction gives $g_J \le 5^J d + B(5^J - 1)/4$, and since $B = o(d)$,

$$d \;\le\; g_j \;\le\; K_J d \qquad (0 \le j \le J), \qquad K_J := 2 \cdot 5^J, \tag{41}$$

for all sufficiently large $d$. Thus $1 \le a_j \le 4K_J d/B + 1 \le Bt_{j-1}$, since $B \to \infty$ and $t_{j-1} \ge d$. The final nominal class size satisfies $\log n_J = g_J = \Theta_\beta(d)$.

### 7.2 Bounding the errors

By (34), together with $a_j \ge 4g_{j-1}/B$, $Bt_{j-1} \le \tau$ and $g_{j-1} \ge d$,

$$\alpha_j \;\le\; \sqrt{2}\,(\tau+1)\,2^{g_{j-1}/(B+1) - 2g_{j-1}/B} \;\le\; \sqrt{2}\,(\tau+1)\,2^{-d/B}. \tag{42}$$

By (31) and $q = B$,

$$\tau = d\big[1 + B(B-1)\big]^J \sim dB^{2J} \sim d^{1+2J\theta} = d^{1/\beta}. \tag{43}$$

Because $\theta < 1$, we have $\log \tau = o(d/B)$. Hence for every fixed $C > 0$ and every $Q \le \tau^C$,

$$\tau^2 Q \max_j \alpha_j \;\le\; \sqrt{2}\,\tau^{C+2}(\tau+1)\,2^{-d/B} = o(1). \tag{44}$$

For the overlap probability, use $a_j \le 4K_J d/B + 1$, $g_{j-1} \le K_J d$ and $t_{j-1} \ge d$,

$$a_j + g_{j-1} - Bt_{j-1} \;\le\; K_J d + \frac{4K_J d}{B} + 1 - Bd = -\Omega(Bd),$$

so (37) gives

$$\zeta \;\le\; \tau\, 2^{-\Omega(Bd)} = o(1/\tau). \tag{45}$$

Combining (35), (44) and (38), every learner making at most $\tau^C$ queries incurs, under the distribution conditioned on no overlaps,

$$\mathbb{E}[M_\tau \mid \mathcal{E}] \;\ge\; \frac{dB^J}{2} - o(1). \tag{46}$$

Since $\tau \sim dB^{2J}$ and $\log n_J = \Theta_\beta(d)$, this is $\Omega_\beta(\sqrt{\tau \log n_J})$.

### 7.3 Prescribing the horizon and the class size exactly

We now pad the conditioned construction to obtain each sufficiently large $T$ and exactly $N = 2^{\lfloor T^\beta \rfloor}$ traces as in Theorem 1.1. Set $c_0 := 1/(2K_J) = 1/(4 \cdot 5^J)$ and run the construction with

$$d = \lfloor c_0 T^\beta \rfloor.$$

By (41) and (43), $\tau \sim c_0^{1/\beta} T$ and $g_J \le K_J c_0 T^\beta = T^\beta/2$; hence, for all sufficiently large $T$,

$$\tau + 1 \le T, \qquad g_J < \lfloor T^\beta \rfloor, \qquad \tau = \Theta_\beta(T). \tag{47}$$

For each trace $h$ in the unpadded class, include the padded trace $(0, h, 0^{T-\tau-1})$, where $0^k$ denotes a string of $k$ zeros. Include also the lexicographically first $N - n_J$ traces of the form $(1, z)$ with $z \in \{0,1\}^{T-1}$. There are enough such traces since $N \le 2^{T-1}$ for large $T$. The two sets are disjoint by their first bit, so the padded class has exactly $N$ traces. Its target is $(0, h^\star, 0^{T-\tau-1})$, where $h^\star$ is the unpadded target.

It remains to show that padding does not make the prediction problem easier. Given a learner for the padded class, we construct a learner for the original class that simulates its interaction. For each padded ERM query $w \in \mathbb{R}^T$, the simulator queries the original oracle with $(w_2, \dots, w_{\tau+1})$ to find the best trace beginning with 0. It computes the best trace beginning with 1 directly, since the added hypotheses are fixed and known. Comparing their scores and applying lexicographic tie-breaking reproduces the padded oracle's answer exactly. Thus, each padded query requires at most one query to the original oracle.

The simulator also supplies the known zero labels outside the original $\tau$ coordinates and uses the observed labels of $h^\star$ for the remaining rounds. Its predictions on these $\tau$ coordinates coincide with those of the padded learner. Hence, its mistake count equals the padded learner's mistake count on the original coordinates, and the padding preserves the expected mistake lower bound without increasing the query budget.

*Proof of Theorem 1.1.* A padded learner making at most $T^C$ queries induces an unpadded learner with the same cap. By (47), $T^C \le \tau^{C+1}$ for all sufficiently large $T$, so (46) applies with exponent $C+1$. Since $B = (1+o(1))\, d^\theta$ and $d = (1+o(1))\, c_0 T^\beta$,

$$dB^J = (1+o(1))\, d^{(1+\beta)/(2\beta)} = (1+o(1))\, c_0^{(1+\beta)/(2\beta)}\, T^{(1+\beta)/2},$$

while $\sqrt{T \log N} = \sqrt{T \lfloor T^\beta \rfloor} \le T^{(1+\beta)/2}$. Thus under the padded distribution,

$$\mathbb{E}[M_T] \;\ge\; c_\beta \sqrt{T \log N}, \qquad c_\beta := \tfrac{1}{4}\, c_0^{(1+\beta)/(2\beta)},$$

for all sufficiently large $T$. The constant $c_\beta$ is independent of $C$. For each learner, averaging gives a fixed pair $(\mathcal{H}, h^\star)$ with exactly $N$ traces on which the same bound holds in expectation over the learner's randomness. □

*Remark* 7.1 (Larger query budgets). The composition error in (44) is the only term in the lower bound that depends on the query budget. Since $\log \tau = o(d/B)$, the error is still $o(1)$ when $Q \le 2^{d/(2B)}$. After padding, $d/B = \Theta_{\beta,J}(T^{\beta-(1-\beta)/(2J)})$, and each padded query still costs one query. Given $\varepsilon > 0$, choose $J$ with $(1-\beta)/(2J) < \min\{\beta, \varepsilon\}$. The same construction then gives the lower bound of Theorem 1.1 for budgets of up to $2^{T^{\beta-\varepsilon}}$ queries, with a positive constant depending on $\beta$ and $\varepsilon$. At a budget of $2TN$ queries, enumeration followed by halving achieves $\log N$ mistakes (Remark 10.2).

## 8 Separating halving from weighted ERM for small classes

We now show that the separation persists even when the hypothesis class is much smaller, with $\log N = \Theta((\log T)^2)$. Unlike Theorem 1.1, the following result is established along a sequence of horizons and class sizes.

**Theorem 8.1** (Separation for small classes)**.** *There are sequences of horizon and class-size pairs $(T_i, N_i)_{i\ge 1}$ with $T_i \to \infty$ of both kinds described below. Fix such a sequence and $C > 0$. For all sufficiently large $i$, every randomized learner $\mathcal{A}$ making at most $T_i^C$ weighted-ERM queries on every execution has a hard instance satisfying the stated lower bound. Here a hard instance consists of a class $\mathcal{H} \subseteq \{0,1\}^{T_i}$ of exactly $N_i$ distinct traces and a target $h^\star \in \mathcal{H}$.*

*(a) For every $\eta \in (0, 1/2)$, the sequence has $\log N_i = O((\log T_i)^p)$ for some $p = p(\eta) < \infty$, and*

$$\mathbb{E}_{\mathcal{A}}[M_{T_i}] \;\ge\; T_i^{1/2-\eta}.$$

*(b) The sequence has $\log N_i = \Theta((\log T_i)^2)$, and for some absolute constant $c > 0$,*

$$\mathbb{E}_{\mathcal{A}}[M_{T_i}] \;\ge\; 2^{c \log T_i / \log\log T_i}. \tag{48}$$

*Proof.* We let the recursion depth $J$ grow with the horizon. The factor $K_J$ in the fixed-depth estimate $g_J \le K_J d$ grows exponentially in $J$, so we bound the nominal log class size $g_J$ directly from (33).

**Part (a).** Fix a constant $\kappa > 0$ and let $J \to \infty$. Choose

$$q = \lceil J^\kappa \rceil, \quad B = \text{the least odd integer } \ge 32Jq, \quad d = \left\lceil J\big(\log(2Jq)\big)^2 \right\rceil, \quad a_j = d \text{ for all } j. \tag{49}$$

Since $t_{j-1} \ge d$, the comparison-set exponent $a_j = d$ satisfies $1 \le a_j \le Bt_{j-1}$. By (33), $g_{j-1} \le d + (j-1)((q-1)d+1) \le d + Jq(d+1)$. Because $B \ge 32Jq$, this implies $g_{j-1}/(B+1) \le d/16$ for large $J$. Substituting into (34) and using $Bt_{j-1} \le \tau$ gives

$$\alpha_j \;\le\; \sqrt{2}\,(\tau+1)\,2^{-7d/16}. \tag{50}$$

The horizon formula (31) and the class-size bounds (33) give

$$\log\tau = \log d + J\log\big(1 + (q-1)B\big) = (2\kappa + 1 + o(1))\, J\log J, \tag{51}$$

$$g_J = \Theta(Jqd) = \Theta\big(J^{\kappa+2}(\log J)^2\big). \tag{52}$$

In particular, $\log\tau = o(d)$ and $g_J = O((\log\tau)^{\kappa+2})$. By (50), the composition error in (35) is $\tau^2 Q \max_j \alpha_j = o(1)$ for every budget $Q \le \tau^C$ with $C$ fixed.

To obtain exactly $n_J$ traces, we condition on the event $\mathcal{E}$ of no overlaps from Section 6.3. Since $a_j + g_{j-1} - Bt_{j-1} \le d + (B+1)d/16 - Bd = -\Omega(Bd)$, (37) gives $\zeta \le \tau 2^{-\Omega(Bd)} = o(1/\tau)$. By (35) and (38), every learner with budget $Q \le \tau^C$ thus satisfies

$$\mathbb{E}[M_\tau \mid \mathcal{E}] \;\ge\; \frac{dq^J}{2} - o(1).$$

The growth exponent of $dq^J$ in the horizon satisfies

$$\frac{\log(dq^J)}{\log\tau} \;\longrightarrow\; \frac{\kappa}{2\kappa+1}. \tag{53}$$

Given $\eta \in (0, 1/2)$, choose $\kappa$ large enough that $\kappa/(2\kappa+1) > 1/2 - \eta$. The lower bound then exceeds $\tau^{1/2-\eta}$ for all sufficiently large $J$, while $\log n_J = O((\log\tau)^p)$ with $p = \kappa + 2$. Taking $(\tau, n_J)$ as the sequence of horizon and size pairs and averaging over the conditioned distribution yields a fixed hard instance for each learner.

**Part (b).** Now take $q = 2$ and keep the definitions of $B$, $d$ and $a_j$ in (49). The same estimates for $\alpha_j$ and $\zeta$ apply, and the horizon and log class size now satisfy

$$\log \tau = \Theta(J \log J), \qquad g_J = \Theta(Jd) = \Theta\big(J^2(\log J)^2\big) = \Theta\big((\log \tau)^2\big).$$

For every fixed $C$ the conditional mistake lower bound is $d2^{J-1} - o(1)$. Since $J = \Theta(\log \tau / \log\log \tau)$, this is at least $2^{c \log \tau / \log\log \tau}$ for some absolute constant $c > 0$ and all sufficiently large $J$. Averaging on $\mathcal{E}$ gives a fixed hard instance with horizon $\tau$ and exactly $n_J$ traces for each learner. □

# 9 Related work

**Transductive online prediction.** The transductive online learning model, in which the instance sequence is known in advance, was studied by Ben-David et al. (1997); Kakade and Kalai (2005) consider a related variant in which only the instance set, rather than its order, is known. For a finite realizable class of size $N$, the classical halving algorithm makes at most $\log_2 N$ mistakes when the consistent hypotheses can be counted (Barzdin and Freivald, 1972; Angluin, 1988; Littlestone, 1988). Random playout and randomized rounding achieve the agnostic-regret rate $O(\sqrt{T \log N})$ using $O(T)$ optimization calls (Cesa-Bianchi and Shamir, 2011, 2013; Rakhlin et al., 2012). Related work characterizes transductive mistake bounds in terms of VC and Littlestone dimensions for explicitly represented hypothesis classes (Hanneke et al., 2023; Chase et al., 2025). In contrast, our results establish the limitations of optimization-oracle access: even polynomially many weighted-ERM queries cannot recover the logarithmic mistake bound of halving.

**Oracle complexity of realizable learning.** Consistency and ERM oracles for online learning have been studied by Assos et al. (2023); Kozachinskiy and Steifer (2024); Daskalakis and Golowich (2024). The closest results in the transductive setting are due to Attias et al. (2025). They study ERM queries on labeled examples and a weaker consistency oracle that reports whether a labeled sample is realizable. Their lower bounds apply to deterministic learners making fewer than $T/2$ ERM queries, and to randomized learners making at most $T/20$ weak-consistency queries. In contrast, Theorem 1.1 covers randomized learners making *any fixed polynomial* number of queries to a stronger weighted-ERM oracle, which accepts arbitrary signed real objectives and returns an entire maximizing hypothesis.

Attias et al. (2025) also ask whether randomized learners can achieve $O(d_{\mathrm{LD}})$ or $O(d_{\mathrm{VC}} \log T)$ mistakes using $T^C 2^{O(d_{\mathrm{VC}})}$ queries, where $d_{\mathrm{LD}}$ and $d_{\mathrm{VC}}$ denote the Littlestone and VC dimensions and $C$ is independent of the class. Our lower bound establishes that a dimension-dependent enlargement of a polynomial query budget is necessary for such guarantees in general. Indeed, the hard classes in Theorem 1.1 have $d_{\mathrm{VC}} = \Theta_\beta(T^\beta)$: their projection onto the coordinates of an initial $d$-dimensional full cube is the whole cube, with $d = \Theta_\beta(T^\beta)$, and $d_{\mathrm{VC}} \le \log_2 N$. Therefore their $\Omega_\beta(T^{(1+\beta)/2})$ expected mistake lower bound exceeds $O(d_{\mathrm{VC}} \log T)$ for every fixed $\beta < 1$. The budget $T^C 2^{O(d_{\mathrm{VC}})}$ can, however, be exponentially larger than a polynomial in $T$ on these classes, so the dimension-dependent question concerns a different query-budget regime. Oracle selection rules have also been studied by Li (2026), while Attias et al. (2026) consider agnostic, non-transductive learning.

**Online algorithms from optimization.** Follow-the-Perturbed-Leader (FTPL) and related methods use offline optimization oracles to construct online learning algorithms (Kalai and Vempala, 2005; Syrgkanis et al., 2016; Dudík et al., 2020). Lower bounds on the power of optimization-oracle access in related settings have been established by Hazan and Koren (2016) and Block et al. (2022). On the positive side, small-loss oracle-efficient algorithms (Wang et al., 2022; Block and Shetty, 2025) demonstrate that additional structural assumptions can lead to stronger guarantees in realizable settings. For arbitrary finite trace classes, however,

the first-order bounds of Wang et al. (2022) still contain an additive term of agnostic order. Our lower bound shows that this dependence is unavoidable in general, even with polynomially many weighted-ERM queries.

**Restricted instance generation.** Under i.i.d., hybrid, or smoothed assumptions, the instance sequences possess additional structure that optimization-based algorithms can exploit (Lazaric and Munos, 2012; Wu et al., 2024; Okoroafor et al., 2026; Buzaglo and Hazan, 2026; Haghtalab et al., 2022; Block et al., 2024). In contrast, we study worst-case transductive online learning, where the instance sequence is known in advance but no distributional or smoothness assumptions are imposed. The main analytic tool in our proof is Boolean hypercontractivity (Bonami, 1970; Beckner, 1975; O'Donnell, 2014), for which we provide a self-contained proof of the required inequality in Section A.

## 10 Discussion and open problems

For $N = 2^{\lfloor T^\beta \rfloor}$ with any fixed $\beta \in (0, 1)$, our results establish that the worst-case realizable mistake bound achievable with polynomially many weighted-ERM queries is $\Theta(\sqrt{T \log N})$, matching the agnostic rate despite the $\log_2 N$ mistake bound of halving with explicit class access. The separation persists for much smaller classes, although the optimal polynomial-query mistake bound in that regime remains open. The key mechanism is the composition lemma (Lemma 5.2), which hides each new prediction problem behind a fixed comparison set, preserving its additive contribution to the mistake lower bound while introducing its hypotheses at only one realized prefix.

*Remark* 10.1 (Expected query budgets). Our lower bounds also apply, up to an additive constant, to learners whose *expected* number of queries is at most $Q$ on every instance. Indeed, stopping such a learner after $TQ$ queries, and predicting 0 on all remaining rounds without further queries, yields a $TQ$-query learner; by Markov's inequality, this changes the expected number of mistakes by at most $T \cdot \mathbb{P}(\text{more than } TQ \text{ queries}) \le 1$.

*Remark* 10.2 (Some restriction is necessary). A weighted-ERM query can determine whether a given prefix $z \in \{0, 1\}^k$ extends to a hypothesis in $\mathcal{H}$. Indeed, set $w_i = 2z_i - 1$ for $i \le k$ and $w_i = 0$ otherwise. Then

$$\langle w, h \rangle = \|z\|_1 - |\{i \le k : h_i \ne z_i\}|,$$

so the optimal value equals $\|z\|_1$ if and only if some $h \in \mathcal{H}$ agrees with $z$ on the first $k$ coordinates. By exploring the tree of extendable prefixes, as in Attias et al. (2025, Lemma 4.1), we can recover the entire class using at most $2TN$ queries: at each depth, there are at most $N$ extendable prefixes, each with two possible extensions. Once $\mathcal{H}$ is recovered, halving achieves at most $\log_2 N$ mistakes. Thus, when $N$ is polynomial in $T$, polynomially many weighted-ERM queries suffice to match halving. More generally, a restriction on the query budget is essential for any separation.

**Open questions.** For classes with $\log N = \Theta((\log T)^2)$, our lower bound is $\exp(\Omega(\log T / \log\log T))$, while random playout achieves $O(\sqrt{T} \log T)$. Closing this gap remains an open problem. Another question is to characterize the tradeoff between the number of oracle queries and the achievable mistake bound, bridging the lower bound in Remark 7.1 and the enumeration upper bound above. Finally, it would be interesting to identify structural assumptions on the hypothesis class or additional oracle capabilities under which logarithmic mistake bounds become achievable with polynomially many queries.

## Statement on the Use of AI Tools

AI systems made substantial contributions to this research, which we disclose here for transparency. Initial investigations with OpenAI's GPT-5.6 Sol and Anthropic's Fable 5 did not resolve the problem. OpenAI's GPT-6 Astra subsequently established a weaker lower bound of order $\Omega(\log N \cdot \log T)$. The main lower bound and its proof presented in this paper were developed by GPT-6.2 Astra. The author formulated the research problem, guided the investigation, and independently verified the mathematical arguments. Claude Code and Codex assisted with manuscript preparation and editing. The author assumes full responsibility for the correctness and content of the paper.

## A An elementary proof of the hypercontractive inequality

For completeness, we prove the only form of hypercontractivity used in Lemma 3.1, following the standard route of a one-bit inequality, tensorization and duality, as in Bonami (1970) (cf. O'Donnell, 2014, Sections 9.3–9.4). Identify $\{0,1\}$ with $\{-1,+1\}$ via $x \mapsto (-1)^x$; this preserves the uniform measure, the Fourier coefficients and all $L_p$ norms, and turns the characters $\chi_U$ into monomials. Let $B = 2\ell - 1 \geq 3$ be odd and $\rho = B^{-1/2}$, and let $\mathrm{T}_\rho$ multiply the Fourier coefficient indexed by $U$ by $\rho^{|U|}$. We prove that, for every $f : \{-1,+1\}^r \to \mathbb{R}$,

$$\|\mathrm{T}_\rho f\|_2 \;\leq\; \|f\|_{1+1/B}. \tag{54}$$

**One bit.** For real $a, b$, a uniformly random sign $\sigma$, and $\ell \geq 2$,

$$\mathbb{E}_\sigma \left| a + \frac{\sigma b}{\sqrt{2\ell - 1}} \right|^{2\ell} \;\leq\; (a^2 + b^2)^\ell. \tag{55}$$

Indeed, the odd powers of $\sigma$ average to zero, so the left-hand side equals

$$\sum_{i=0}^{\ell} \binom{2\ell}{2i} \frac{a^{2\ell-2i} b^{2i}}{(2\ell-1)^i}.$$

For every $0 \leq i \leq \ell$,

$$\binom{2\ell}{2i} \;\leq\; \binom{\ell}{i} (2\ell-1)^i. \tag{56}$$

To see this, note that the ratio of the left-hand side to $\binom{\ell}{i}$ equals, with the convention $(-1)!! = 1$,

$$\frac{(2\ell-1)!!}{(2i-1)!!\,(2\ell-2i-1)!!} = \frac{\prod_{j=0}^{i-1}(2\ell-2j-1)}{(2i-1)!!} \;\leq\; (2\ell-1)^i.$$

Substituting (56) and applying the binomial theorem yields (55).

**Tensorization.** We prove by induction on $r$ the dual estimate $\|\mathrm{T}_\rho u\|_{2\ell} \leq \|u\|_2$. The case $r = 0$ is trivial. Write a function of $r$ signs as $u(z,\sigma) = a(z) + \sigma b(z)$, where $z$ denotes the first $r-1$ signs, and let $\tilde{a} = \mathrm{T}_\rho a$ and $\tilde{b} = \mathrm{T}_\rho b$, with the noise operator acting on the first $r-1$ coordinates. Then $\mathrm{T}_\rho u(z,\sigma) = \tilde{a}(z) + \rho\sigma\tilde{b}(z)$. Applying (55) pointwise, then Minkowski's inequality in $L_\ell$, and then the induction hypothesis,

$$\begin{aligned} \|\mathrm{T}_\rho u\|_{2\ell}^2 &= \left( \mathbb{E}_z \mathbb{E}_\sigma \left| \tilde{a}(z) + \rho\sigma\tilde{b}(z) \right|^{2\ell} \right)^{1/\ell} \leq \left( \mathbb{E}_z \left( \tilde{a}(z)^2 + \tilde{b}(z)^2 \right)^\ell \right)^{1/\ell} \\ &\leq \|\tilde{a}\|_{2\ell}^2 + \|\tilde{b}\|_{2\ell}^2 \leq \|a\|_2^2 + \|b\|_2^2 = \|u\|_2^2. \end{aligned}$$

This proves $\|\mathrm{T}_\rho u\|_{2\ell} \leq \|u\|_2$ on every Boolean cube.

**Duality.** The operator $\mathrm{T}_\rho$ is self-adjoint with respect to the uniform measure, and $p = 1 + 1/B$ has conjugate exponent $p' = B + 1 = 2\ell$. For every $f$, by Hölder's inequality and the tensorized bound,

$$\|\mathrm{T}_\rho f\|_2 = \sup_{\|u\|_2 \le 1} \mathbb{E}\big[(\mathrm{T}_\rho f)\, u\big] = \sup_{\|u\|_2 \le 1} \mathbb{E}\big[f\, \mathrm{T}_\rho u\big] \le \|f\|_p \sup_{\|u\|_2 \le 1} \|\mathrm{T}_\rho u\|_{p'} \le \|f\|_p,$$

which is (54).

## References


Dana Angluin. Queries and concept learning. *Machine Learning*, 2(4):319–342, 1988. doi:10.1007/BF00116828.

Angelos Assos, Idan Attias, Yuval Dagan, Constantinos Daskalakis, and Maxwell K. Fishelson. Online learning and solving infinite games with an ERM oracle. In *Proceedings of Thirty Sixth Conference on Learning Theory*, volume 195 of *Proceedings of Machine Learning Research*, pages 274–324, 2023. URL https://proceedings.mlr.press/v195/assos23a.html.

Idan Attias, Steve Hanneke, and Arvind Ramaswami. Tradeoffs between mistakes and ERM oracle calls in online and transductive online learning. In *Advances in Neural Information Processing Systems*, volume 38, 2025. doi:10.52202/085713-2542.

Idan Attias, Steve Hanneke, and Arvind Ramaswami. Regret–oracle complexity tradeoffs in agnostic online learning. arXiv:2605.07155, 2026.

J. M. Barzdin and R. V. Freivald. On the prediction of general recursive functions. *Soviet Mathematics Doklady*, 13:1224–1228, 1972. English translation of *Doklady Akademii Nauk SSSR*, 206(3):521–524, 1972.

William Beckner. Inequalities in Fourier analysis. *Annals of Mathematics*, 102(1):159–182, 1975. doi:10.2307/1970980.

Shai Ben-David, Eyal Kushilevitz, and Yishay Mansour. Online learning versus offline learning. *Machine Learning*, 29(1):45–63, 1997. doi:10.1023/A:1007465907571.

Adam Block and Abhishek Shetty. Small loss bounds for online learning separated function classes: A Gaussian process perspective. arXiv:2502.10292, 2025.

Adam Block, Yuval Dagan, Noah Golowich, and Alexander Rakhlin. Smoothed online learning is as easy as statistical learning. In *Proceedings of Thirty Fifth Conference on Learning Theory*, volume 178 of *Proceedings of Machine Learning Research*, pages 1716–1786, 2022. URL https://proceedings.mlr.press/v178/block22a.html.

Adam Block, Alexander Rakhlin, and Abhishek Shetty. On the performance of empirical risk minimization with smoothed data. In *Proceedings of Thirty Seventh Conference on Learning Theory*, volume 247 of *Proceedings of Machine Learning Research*, pages 596–629, 2024. URL https://proceedings.mlr.press/v247/block24a.html.

Aline Bonami. Étude des coefficients de Fourier des fonctions de $L^p(G)$. *Annales de l'Institut Fourier*, 20 (2):335–402, 1970. doi:10.5802/aif.357.

Léon Bottou, Frank E. Curtis, and Jorge Nocedal. Optimization methods for large-scale machine learning. *SIAM Review*, 60(2):223–311, 2018. doi:10.1137/16M1080173.

Gon Buzaglo and Elad Hazan. Oracle-efficient online classification with stochastic inputs and adversarial outputs. arXiv:2609.33760, 2026.

Nicolò Cesa-Bianchi and Ohad Shamir. Efficient online learning via randomized rounding. In *Advances in Neural Information Processing Systems*, volume 24, pages 343–351, 2011. URL https://papers.nips.cc/paper_files/paper/2011/hash/3cec07e9ba5f5bb252d13f5f431e4bbb-Abstract.html.

Nicolò Cesa-Bianchi and Ohad Shamir. Efficient transductive online learning via randomized rounding. In Bernhard Schölkopf, Zhiyuan Luo, and Vladimir Vovk, editors, *Empirical Inference: Festschrift in Honor of Vladimir N. Vapnik*, pages 177–194. Springer, 2013. doi:10.1007/978-3-642-41136-6_16.

Zachary Chase, Steve Hanneke, Shay Moran, and Jonathan Shafer. Optimal mistake bounds for transductive online learning. In *Advances in Neural Information Processing Systems*, volume 38, 2025. doi:10.52202/085713-5090.

Constantinos Daskalakis and Noah Golowich. Is efficient PAC learning possible with an oracle that responds "yes" or "no"? In *Proceedings of Thirty Seventh Conference on Learning Theory*, volume 247 of *Proceedings of Machine Learning Research*, pages 1263–1307, 2024. URL https://proceedings.mlr.press/v247/daskalakis24a.html.

Miroslav Dudík, Nika Haghtalab, Haipeng Luo, Robert E. Schapire, Vasilis Syrgkanis, and Jennifer Wortman Vaughan. Oracle-efficient online learning and auction design. *Journal of the ACM*, 67(5): 26:1–26:57, 2020. doi:10.1145/3402203.

Nika Haghtalab, Yanjun Han, Abhishek Shetty, and Kunhe Yang. Oracle-efficient online learning for smoothed adversaries. In *Advances in Neural Information Processing Systems*, volume 35, pages 4072–4084, 2022. doi:10.52202/068431-0294.

Steve Hanneke, Shay Moran, and Jonathan Shafer. A trichotomy for transductive online learning. In *Advances in Neural Information Processing Systems*, volume 36, pages 19502–19519, 2023. doi:10.52202/075280-0856.

Elad Hazan and Tomer Koren. The computational power of optimization in online learning. In *Proceedings of the 48th Annual ACM Symposium on Theory of Computing (STOC)*, pages 128–141, 2016. doi:10.1145/2897518.2897536.

Sham Kakade and Adam Tauman Kalai. From batch to transductive online learning. In *Advances in Neural Information Processing Systems*, volume 18, pages 611–618, 2005. URL https://papers.nips.cc/paper_files/paper/2005/hash/17693c91d9204b7a7646284bb3adb603-Abstract.html.

Adam Kalai and Santosh Vempala. Efficient algorithms for online decision problems. *Journal of Computer and System Sciences*, 71(3):291–307, 2005. doi:10.1016/j.jcss.2004.10.016.

Alexander Kozachinskiy and Tomasz Steifer. Simple online learning with consistent oracle. In *Proceedings of Thirty Seventh Conference on Learning Theory*, volume 247 of *Proceedings of Machine Learning Research*, pages 3241–3256, 2024. URL https://proceedings.mlr.press/v247/kozachinskiy24a.html.

Alessandro Lazaric and Rémi Munos. Learning with stochastic inputs and adversarial outputs. *Journal of Computer and System Sciences*, 78(5):1516–1537, 2012. doi:10.1016/j.jcss.2011.12.027.

Xuan Li. An exponential deterministic–randomized gap in ERM-oracle complexity for thresholds on an unknown order. arXiv:2609.10196, 2026.

Nick Littlestone. Learning quickly when irrelevant attributes abound: A new linear-threshold algorithm. *Machine Learning*, 2(4):285–318, 1988. doi:10.1007/BF00116827.

Ryan O'Donnell. *Analysis of Boolean Functions*. Cambridge University Press, 2014. doi:10.1017/CBO9781139814782.

Princewill Okoroafor, Robert Kleinberg, and Michael P. Kim. Oracle-efficient hybrid learning with constrained adversaries. In *The Fourteenth International Conference on Learning Representations (ICLR)*, 2026. URL https://proceedings.iclr.cc/paper_files/paper/2026/hash/55a2ee298e110ce49d8a21e3ee4c6f2e-Abstract-Conference.html.

Alexander Rakhlin, Ohad Shamir, and Karthik Sridharan. Relax and randomize: From value to algorithms. In *Advances in Neural Information Processing Systems*, volume 25, pages 2141–2149, 2012. URL https://papers.nips.cc/paper_files/paper/2012/hash/53adaf494dc89ef7196d73636eb2451b-Abstract.html.

Norbert Sauer. On the density of families of sets. *Journal of Combinatorial Theory, Series A*, 13(1): 145–147, 1972. doi:10.1016/0097-3165(72)90019-2.

Vasilis Syrgkanis, Akshay Krishnamurthy, and Robert E. Schapire. Efficient algorithms for adversarial contextual learning. In *Proceedings of the 33rd International Conference on Machine Learning*, volume 48 of *Proceedings of Machine Learning Research*, pages 2159–2168, 2016. URL https://proceedings.mlr.press/v48/syrgkanis16.html.

Guanghui Wang, Zihao Hu, Vidya Muthukumar, and Jacob D. Abernethy. Adaptive oracle-efficient online learning. In *Advances in Neural Information Processing Systems*, volume 35, pages 23398–23411, 2022. doi:10.52202/068431-1700.

Changlong Wu, Jin Sima, and Wojciech Szpankowski. Oracle-efficient hybrid online learning with unknown distribution. In *Proceedings of Thirty Seventh Conference on Learning Theory*, volume 247 of *Proceedings of Machine Learning Research*, pages 4992–5018, 2024. URL https://proceedings.mlr.press/v247/wu24a.html.