Introduction to Coding Theory **Técnico–ULisboa, 2026/2027**

Part 10: MacWilliams identities and the MRRW bounds

Lecturer: João Ribeiro

Introduction

We now return to the basic problem of understanding how large we can make the rate of a binary code $\mathcal{C} \subseteq \mathbb{F}_2^n$ with relative distance δ. We are interested in understanding this question in the asymptotic regime as $n \to \infty$. We have already seen some upper bounds (Hamming, Singleton, Elias–Bassalygo) and a lower bound (Gilbert–Varshamov). In these notes we will discuss one of the best known rate upper bounds – the first MRRW bound, due to McEliece, Rodemich, Rumsey, and Welch in 1970s. We will not follow the original proof. Instead, we will follow a later alternative proof due to Navon and Samorodnitsky, and we will only present the argument for binary *linear* codes. This will require developing some basic concepts from the analysis of boolean functions, and along the way we will use these concepts to give a nice proof of the MacWilliams identities relating the weight distributions of a linear code and its dual.

Loosely speaking, the first MRRW bound can be seen as a specific instantiation of a general linear programming framework that yields more types of "MRRW bounds". These MRRW bounds stood as the best rate upper bounds for nearly 50 years. In August 2026, breakthrough works of Alrabiah–Guruswami and OpenAI managed to improve on the MRRW bounds for the first time.

1 Basics of boolean functional analysis

We begin by developing the required concepts from the analysis of boolean functions. If you would like to learn more about this, check out Ryan O'Donnell's excellent book.

Consider the space of functions $f : \mathbb{F}_2^n \to \mathbb{R}$ with the inner product

$$\langle f, g \rangle = 2^{-n} \sum_{x \in \mathbb{F}_2^n} f(x) \cdot g(x) = \mathrm{E}_{x \sim \mathbb{F}_2^n}[f(x) \cdot g(x)],$$

which is a renormalization of the usual inner product between functions that will simplify expressions later on. Above, $x \sim \mathbb{F}_2^n$ means that x is sampled uniformly at random from $\mathbb{F}_2^n$.

There is an obvious "basis" of 2^n functions for this space. Indeed, for each $\alpha \in \mathbb{F}_2^n$ define the function

$$e_\alpha(x) = \begin{cases} 2^{n/2}, & \text{if } x = \alpha, \\ 0, & \text{otherwise.} \end{cases}$$

This is a collection of 2^n orthonormal functions, and every $f : \mathbb{F}_2^n \to \mathbb{R}$ can be written uniquely as an $\mathbb{R}$-linear combination of the e_α's, since

$$f(x) = \sum_{\alpha \in \mathbb{F}_2^n} f(\alpha) \cdot 2^{-n/2} e_\alpha(x) = \sum_{\alpha \in \mathbb{F}_2^n} \langle f, e_\alpha \rangle \cdot e_\alpha(x)$$

for all $x \in \mathbb{F}_2^n$.

It turns out that writing functions in an alternative "Fourier basis" allows us to give nice proofs of many important results. For each $\alpha \in \mathbb{F}_2^n$, consider the function

$$\chi_\alpha(x) = (-1)^{\langle x, \alpha \rangle}$$

with $\langle x, \alpha \rangle = \sum_{i=1}^n x_i \cdot \alpha_i \pmod 2$ the usual inner product in $\mathbb{F}_2^n$.

Theorem 1 *The functions χ_α for $\alpha \in \mathbb{F}_2^n$ form an orthonormal basis of the space of functions $f : \mathbb{F}_2^n \to \mathbb{R}$. Furthermore, every such f can be written uniquely as*

$$f(x) = \sum_{\alpha \in \mathbb{F}_2^n} \widehat{f}(\alpha) \cdot \chi_\alpha(x),$$

with $\widehat{f}(\alpha) = \langle f, \chi_\alpha \rangle$.

Note that $\widehat{f}$ is also a function from $\mathbb{F}_2^n$ to $\mathbb{R}$. We call it the *Fourier transform* of f. We record some basic properties of the Fourier transform below, which you will prove in the problem set.

Theorem 2 (Parseval) *For all $f : \mathbb{F}_2^n \to \mathbb{R}$ we have*

$$\langle f, f \rangle = \sum_{\alpha \in \mathbb{F}_2^n} \widehat{f}(\alpha)^2.$$

Theorem 3 (Plancherel) *For all $f, g : \mathbb{F}_2^n \to \mathbb{R}$ we have*

$$\langle f, g \rangle = \sum_{\alpha \in \mathbb{F}_2^n} \widehat{f}(\alpha) \cdot \widehat{g}(\alpha).$$

We will also need to study the *convolution* of two functions f and g, denoted by $f * g$ and given by

$$(f * g)(x) = \mathrm{E}_{y \sim \mathbb{F}_2^n}[f(y) \cdot g(x - y)].$$

There is a simple identity connecting the Fourier transforms of f and g with that of $f * g$.

Theorem 4 (Fourier transform of the convolution) *For all $f, g : \mathbb{F}_2^n \to \mathbb{R}$ we have*

$$\widehat{f * g}(\alpha) = \widehat{f}(\alpha) \cdot \widehat{g}(\alpha).$$

2 MacWilliams identities

As a warmup, we will use the concepts from the analysis of boolean functions that we just discussed to give a nice proof of the *MacWilliams identities*. These identities allow us to relate the *weight distribution* of a linear code $\mathcal{C} \subseteq \mathbb{F}_2^n$ (i.e., how many codewords are there of each given weight) to the weight distribution of the dual $\mathcal{C}^\perp$.

Definition 1 (Weight distribution of a code) *The* weight distribution *of a code $\mathcal{C} \subseteq \mathbb{F}_2^n$ is the vector $W^{\mathcal{C}} = (W_0^{\mathcal{C}}, W_1^{\mathcal{C}}, \ldots, W_n^{\mathcal{C}})$ with $W_i^{\mathcal{C}} = |\{c \in \mathcal{C} : w_H(c) = i\}|$.*

The following key lemma shows that the Fourier transform of the indicator of a linear code $\mathcal{C}$ is a renormalization of the indicator of its dual.

Lemma 1 *Fix an arbitrary linear code $\mathcal{C} \subseteq \mathbb{F}_2^n$ and let $\mathbf{1}_{\mathcal{C}}$ denote the indicator function of $\mathcal{C}$. Then,*

$$\widehat{\mathbf{1}_{\mathcal{C}}} = \frac{|\mathcal{C}|}{2^n} \cdot \mathbf{1}_{\mathcal{C}^\perp}.$$

Proof: For any $\alpha \in \mathbb{F}_2^n$ we have

$$\widehat{\mathbf{1}_{\mathcal{C}}}(\alpha) = \mathrm{E}_{x \sim \mathbb{F}_2^n}[\mathbf{1}_{\mathcal{C}}(x) \cdot (-1)^{\langle x, \alpha \rangle}] = 2^{-n} \sum_{x \in \mathcal{C}} (-1)^{\langle x, \alpha \rangle}.$$

If $\alpha \in \mathcal{C}^\perp$, then $\langle x, \alpha \rangle = 0$ for all $x \in \mathcal{C}$, in which case

$$\widehat{\mathbf{1}_{\mathcal{C}}}(\alpha) = 2^{-n} \sum_{x \in \mathcal{C}} 1 = \frac{|\mathcal{C}|}{2^n}.$$

Otherwise, if $\alpha \notin \mathcal{C}^\perp$, then there is $x \in \mathcal{C}$ such that $\langle x, \alpha \rangle = 1$. We leave it as a brief exercise for the reader to show that this implies that

$$\sum_{x \in \mathcal{C}} (-1)^{\langle x, \alpha \rangle} = 0,$$

as desired. ∎

We now use Lemma 1 to prove the MacWilliams identities.

Theorem 5 (MacWilliams identities) *Fix an arbitrary linear code $\mathcal{C} \subseteq \mathbb{F}_2^n$. Then,*

$$W_\ell^{\mathcal{C}^\perp} = \frac{1}{|\mathcal{C}|} \sum_{i=0}^{n} W_i^{\mathcal{C}} \cdot K_\ell(i),$$

where $K_\ell(i) = \sum_{j=0}^{i} (-1)^j \binom{i}{j} \binom{n-i}{\ell-j}$ is called the ℓ-th Krawtchouk polynomial.

Proof: We have

$$\begin{aligned} W_\ell^{\mathcal{C}^\perp} &= \sum_{\alpha \in \mathbb{F}_2^n : w_H(\alpha) = \ell} \mathbf{1}_{\mathcal{C}^\perp}(\alpha) \\ &= \frac{2^n}{|\mathcal{C}|} \sum_{\alpha \in \mathbb{F}_2^n : w_H(\alpha) = \ell} \widehat{\mathbf{1}_{\mathcal{C}}}(\alpha) \\ &= \frac{2^n}{|\mathcal{C}|} \sum_{\alpha \in \mathbb{F}_2^n : w_H(\alpha) = \ell} \mathrm{E}_{x \sim \mathbb{F}_2^n}[\mathbf{1}_{\mathcal{C}}(x) \cdot (-1)^{\langle x, \alpha \rangle}] \\ &= \frac{2^n}{|\mathcal{C}|} \mathrm{E}_{x \sim \mathbb{F}_2^n} \left[\mathbf{1}_{\mathcal{C}}(x) \cdot \sum_{\alpha \in \mathbb{F}_2^n : w_H(\alpha) = \ell} (-1)^{\langle x, \alpha \rangle} \right]. \end{aligned} \tag{1}$$

The second equality follows from Lemma 1 and the fourth equality uses linearity of expectation.

Now, we claim that for $x \in \mathcal{C}$ with $w_H(x) = i$ we have

$$\sum_{\alpha \in \mathbb{F}_2^n : w_H(\alpha) = \ell} (-1)^{\langle x, \alpha \rangle} = \sum_{j=0}^{i} (-1)^j \binom{i}{j} \binom{n-i}{\ell - j}.$$

The proof of this claim is left as an exercise. Then, since this quantity only depends on $w_H(x)$ and $w_H(\alpha)$, we can simplify Equation (1) to

$$W_\ell^{\mathcal{C}^\perp} = \frac{1}{|\mathcal{C}|} \sum_{i=0}^{n} W_i^{\mathcal{C}} \sum_{j=0}^{i} (-1)^j \binom{i}{j} \binom{n-i}{\ell - j},$$

as desired. ∎

Note that the MacWilliams identities show in particular that, remarkably, the weight distribution of $\mathcal{C}$ is completely determined solely by the weight distribution of its dual $\mathcal{C}^\perp$.

3 Bounding the size of codes through linear programming

We now shift our focus to our main goal of obtaining better upper bounds on the rate of a binary code with relative distance δ. We start by briefly describing an approach based on linear programming that yields some of the best known upper bounds.

Consider the following linear program:

$$\begin{aligned} \max \quad & \sum_{i=0}^{n} w_i \\ \text{s.t.} \quad & w_0 = 1, \\ & w_1 = \cdots = w_{d-1} = 0, \\ & w_i \geq 0, \forall i \geq d. \end{aligned}$$

Since the weight distribution of any binary linear code $\mathcal{C} \subseteq \mathbb{F}_2^n$ with minimum distance d satisfies the constraints above, the optimal solution to this linear program yields an upper bound on the size of any such code. However, this isn't really a useful linear program, because there are no constraints relating the w_i's.

Instead, inspired by the MacWilliams identities, we consider a more constrained linear program. We know that $\sum_{i=0}^{n} W_i^{\mathcal{C}} \cdot K_\ell(i)$ must be non-negative for every ℓ, since this equals $|\mathcal{C}| \cdot W_\ell^{\mathcal{C}^\perp}$ by the MacWilliams identities. Therefore, we consider the following linear program:

$$\begin{aligned} \max \quad & \sum_{i=0}^{n} w_i \\ \text{s.t.} \quad & w_0 = 1, \\ & w_1 = \cdots = w_{d-1} = 0, \\ & w_i \geq 0, \forall i \in [n], \\ & \sum_{i=0}^{n} w_i \cdot K_\ell(i) \geq 0, \forall \ell \in [n]. \end{aligned}$$

We will not show this here, but it is not too difficult to argue that these constraints are also satisfied by any *non-linear* code (in that case we work with all distances between codewords instead of the weight distribution).

Analyzing this linear program yields some of the best known upper bounds on the size of binary linear error-correcting codes. These bounds are obtained by carefully constructing feasible solutions to the dual program, as done by McEliece, Rodemich, Rumsey, and Welch in the 1970s [MRRW77]. By weak duality, these feasible solutions yield upper bounds on the optimum of the original linear program. We will not deepen this, but instead we will give an alternative proof of a celebrated bound of this type (the *first MRRW bound*, focusing on binary linear codes) through the notion of *covering*, avoiding linear programming and orthogonal polynomials. This alternative proof is due to Navon and Samorodnitsky [NS08], and the exposition in these notes draws heavily from [NS08] and Ta-Shma's 2013 lecture notes (here and here).

4 The first MRRW bound via the essential covering radius

We will prove a rate upper bound for error-correction by studying the dual problem of *covering*. We begin with the standard definition of covering radius, similar to what you already saw in the problem sets.

Definition 2 (Covering radius) *We say that a code $\mathcal{C} \subseteq \mathbb{F}_2^n$ has* covering radius *at most r if*

$$\bigcup_{c \in \mathcal{C}} B_r(c) = \mathbb{F}_2^n.$$

We will instead work with a relaxation of the covering radius. Intuitively, instead of asking for the smallest radius r that lets us cover the whole space with radius-r balls centered at codewords, we ask only that we cover a decent fraction of the space. More precisely, we have the following definition.

Definition 3 (Essential covering radius) *We say that a code $\mathcal{C} \subseteq \mathbb{F}_2^n$ has* essential covering radius *at most r if*

$$\left|\bigcup_{c\in\mathcal{C}} B_r(c)\right| \geq \frac{2^n}{n}.$$

The covering radius and essential covering radius of a linear code $\mathcal{C}$ are related to the distance of its dual $\mathcal{C}^\perp$. More precisely, we will show the following.

Theorem 6 *Let $\mathcal{C}$ be a binary linear code of minimum distance at least $d = \delta n$ with $\delta \in (0, 1/2)$. Then, the essential covering radius of $\mathcal{C}^\perp$ is at most $\left(\frac{1}{2} - \sqrt{\delta(1-\delta)} + o(1)\right) n$.*

The first MRRW bound for binary linear codes follows easily from Theorem 6.

Theorem 7 (First MRRW bound for binary linear codes) *Every binary linear code $\mathcal{C} \subseteq \mathbb{F}_2^n$ of minimum distance at least $d = \delta n$ with $\delta \in (0, 1/2)$ and rate R satisfies*

$$R \leq h\left(\frac{1}{2} - \sqrt{\delta(1-\delta)}\right) + o(1).$$

Proof: By Theorem 6, we know that for $r = \left(\frac{1}{2} - \sqrt{\delta(1-\delta)} + o(1)\right) n$ we have

$$\frac{2^n}{n} \leq \left|\bigcup_{c\in\mathcal{C}^\perp} B_r(c)\right| \leq |\mathcal{C}^\perp| \cdot |B_r(0)| \leq |\mathcal{C}^\perp| \cdot 2^{nh(r/n)}.$$

Rearranging and noting that $|\mathcal{C}| = 2^n/|\mathcal{C}^\perp|$, we conclude that

$$|\mathcal{C}| \leq n \cdot 2^{nh(r/n)} = 2^{\left(h\left(1/2 - \sqrt{\delta(1-\delta)}\right) + o(1)\right) n},$$

as desired. ∎

We will actually study a more general version of the covering problem above. More precisely, consider an arbitrary subset $B \subseteq \mathbb{F}_2^n$. Then, we want to identify conditions on B that allow us to establish that

$$\left|\mathcal{C}^\perp + B\right| \geq \frac{2^n}{n}, \tag{2}$$

where for two sets A and B we define the sumset $A + B = \{a + b : a \in A, b \in B\}$.

We begin by recasting this as a Fourier-analytic problem.

Lemma 2 *Fix an arbitrary set $U \subseteq \mathbb{F}_2^n$. Suppose that there exists a function $F : \mathbb{F}_2^n \to \mathbb{R}$ supported[1] on U such that $\mathrm{E}[F] \neq 0$ and*

$$\frac{\mathrm{E}[F^2]}{\mathrm{E}[F]^2} \leq n.$$

Then, $|U| \geq \frac{2^n}{n}$.

[1] A function f is supported on a set S if $f(x) = 0$ for all $x \notin S$.

Proof: By Cauchy-Schwarz, we have

$$\mathrm{E}[F]^2 = \langle F, \mathbf{1}_U \rangle^2 \leq \langle F, F \rangle \cdot \langle \mathbf{1}_U, \mathbf{1}_U \rangle = \mathrm{E}[F^2] \cdot \frac{|U|}{2^n}.$$

Rearranging, we get that

$$|U| \geq \frac{2^n \, \mathrm{E}[F]^2}{\mathrm{E}[F^2]} \geq \frac{2^n}{n}$$

by the hypothesis on F. ∎

From Lemma 2 we see that to establish Equation (2) it suffices to showcase a function F supported on $\mathcal{C}^\perp + B$ such that

$$\frac{\mathrm{E}[F^2]}{\mathrm{E}[F]^2} \leq n.$$

4.1 Setting things up with spectral graph theory

Our construction of this function F will be motivated by some facts from spectral graph theory. Write $N = 2^n$. Consider an N-vertex graph with $N \times N$ adjacency matrix A. As we have seen before, since A is a symmetric matrix with real-valued entries, the spectral theorem states that A has N not necessarily distinct eigenvalues $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_N$ and orthonormal real-valued vectors $u_1, \ldots, u_N \in \mathbb{R}^N$ such that u_i is an eigenvector of λ_i (i.e., $Au_i = \lambda_i u_i$).

We can learn a lot about a graph by studying the eigenvalues and eigenvectors of its adjacency matrix. The following variational characterization of the largest eigenvalue of A will be useful.

Lemma 3 *We have*

$$\lambda_1 = \max_{v \in \mathbb{R}^N \setminus \{0\}} \frac{\langle Av, v \rangle}{\langle v, v \rangle}.$$

Furthermore, every maximizer v is an eigenvector of λ_1.

Proof: For you in the problem set. ∎

Our discussion will focus on (induced subgraphs of) the *Boolean hypercube graph* G, whose vertices are labeled by elements of $\mathbb{F}_2^n$ and two vertices $x, y \in \mathbb{F}_2^n$ are adjacent if and only if $d(x, y) = 1$. In this case $N = 2^n$, and from here onward we will see vectors $v \in \mathbb{R}^N$ as functions $f : \mathbb{F}_2^n \to \mathbb{R}$. Under this perspective, the y-th entry of Af can be written as

$$(Af)_y = \sum_{i=1}^{n} f(y + e_i) = (f * L)(y)$$

where $L : \mathbb{F}_2^n \to \mathbb{R}$ is given by

$$L(x) = \begin{cases} 2^n, & \text{if } w_H(x) = 1, \\ 0, & \text{otherwise.} \end{cases}$$

All of these perspectives will be useful.

We denote by A_B the adjacency matrix of the subgraph of G induced by the vertices in B and by λ_B its largest eigenvalue. We will prove the following.

Theorem 8 *Let $\mathcal{C}$ be a linear code with minimum distance $d < n/2$ and $B \subseteq \mathbb{F}_2^n$ nonempty. Then, there exists a non-negative and non-zero function F supported on $\mathcal{C}^\perp + B$ such that*

$$\frac{(\lambda_B - (n-2d))\,\mathrm{E}[F^2]}{\mathrm{E}[F]^2} \leq n.$$

In particular, if $\lambda_B \geq n - 2d + 1$, then

$$\left|\mathcal{C}^\perp + B\right| \geq \frac{2^n}{n}.$$

Proof: We construct the desired F as follows. Let $f_B : B \to \mathbb{R}$ be an eigenfunction of λ_B. By Lemma 3, we know that

$$\lambda_B = \frac{\langle A_B f_B, f_B\rangle}{\langle f_B, f_B\rangle}.$$

Define $f : \mathbb{F}_2^n \to \mathbb{R}$ as the extension of f_B to $\mathbb{F}_2^n$ by setting $f(x) = 0$ for all $x \notin B$. Note that since A is non-negative we can choose f_B so that it is non-negative, and in that case we get that

$$Af \geq \lambda_B f.$$

Then, we set

$$F = \mathbf{1}_{\mathcal{C}^\perp} * f.$$

Note that

$$F(x) = (\mathbf{1}_{\mathcal{C}^\perp} * f)(x) = 2^{-n} \sum_{y \in \mathcal{C}^\perp} f(x+y),$$

and so indeed F is supported on $\mathcal{C}^\perp + B$.

We proceed to show that $\mathrm{E}[F^2]/\,\mathrm{E}[F]^2 \leq n$. We will do this by studying $\langle AF, F\rangle$. First, note that

$$AF = (\mathbf{1}_{\mathcal{C}^\perp} * f) * L = \mathbf{1}_{\mathcal{C}^\perp} * (f * L) \geq \lambda_B(\mathbf{1}_{\mathcal{C}^\perp} * f) = \lambda_B F.$$

Therefore,

$$\langle AF, F\rangle \geq \lambda_B \langle F, F\rangle = \lambda_B\,\mathrm{E}[F^2]. \tag{3}$$

On the other hand, by Plancherel, properties of the convolution, and the fact that $\widehat{L}(\alpha) = n - 2w_H(\alpha)$, we have

$$\langle AF, F\rangle = 2^n\langle \widehat{AF}, \widehat{F}\rangle = 2^n\langle \widehat{F}\cdot\widehat{L}, \widehat{F}\rangle = \sum_{\alpha\in\mathbb{F}_2^n} (n - 2w_H(\alpha))\cdot \widehat{F}(\alpha)^2. \tag{4}$$

Now, since $\mathcal{C}$ has minimum distance d, we know that $\widehat{F}(\alpha) = 0$ for all α with $0 < w_H(\alpha) < d$. Therefore,

$$\begin{aligned}
\sum_{\alpha\in\mathbb{F}_2^n} (n - 2w_H(\alpha))\cdot \widehat{F}(\alpha)^2 &= n\widehat{F}(0)^2 + \sum_{\alpha : w_H(\alpha)\geq d} (n - 2w_H(\alpha))\cdot \widehat{F}(\alpha)^2 \\
&\leq n\widehat{F}(0)^2 + \sum_{\alpha : w_H(\alpha)\geq d} (n - 2d)\cdot \widehat{F}(\alpha)^2 \\
&\leq n\,\mathrm{E}[F]^2 + (n-2d)\sum_{\alpha} \widehat{F}(\alpha)^2 \\
&= n\,\mathrm{E}[F]^2 + (n-2d)\,\mathrm{E}[F^2].
\end{aligned} \tag{5}$$

Combining Equations (3) to (5), we get

$$\lambda_B \operatorname{E}[F^2] \leq n \operatorname{E}[F]^2 + (n-2d)\operatorname{E}[F^2],$$

or, equivalently,

$$\frac{(\lambda_B - (n-2d))\operatorname{E}[F^2]}{\operatorname{E}[F]^2} \leq n.$$

■

To obtain Theorem 6 it remains to show that $\lambda_B \geq n - 2d + 1$ for $B = B_r(0)$ a Hamming ball of radius $r = (\frac{1}{2} - \sqrt{\delta(1-\delta)} + o(1))n$ and $d = \delta n$, and then invoke Lemma 2 and Theorem 8. This is a consequence of the following lemma.

Lemma 4 *For $r = \rho n$ with $\rho \in (0, 1/2)$ we have*

$$\lambda_{B_r(0)} \geq 2\sqrt{r(n-r)} - o(n).$$

Further reading

In very recent concurrent breakthroughs, Alrabiah and Guruswami [AG26] and OpenAI [Ope26] improved slightly on the MRRW bounds. Notably, Alrabiah and Guruswami present a new framework for rate upper bounds that recovers all previous bounds and improves on the MRRW bound by relating rate upper bounds to the analysis of *probabilistic channels* binary input/quantum output channels. If you are interested in reading more about this and how the two concurrent results above relate to each other, see Barg's note [Bar26].

References

[AG26] Omar Alrabiah and Venkatesan Guruswami. Binary code rate bounds via classical–quantum channels, August 2026. https://arxiv.org/abs/2608.09347.

[Bar26] Alexander Barg. Comments on the recent improvements of the MRRW bounds, September 2026. https://arxiv.org/abs/2609.01860v1.

[MRRW77] R. McEliece, E. Rodemich, H. Rumsey, and L. Welch. New upper bounds on the rate of a code via the Delsarte-MacWilliams inequalities. *IEEE Transactions on Information Theory*, 23(2):157–166, 1977.

[NS08] Michael Navon and Alex Samorodnitsky. Linear programming bounds for codes via a covering argument. *Discrete & Computational Geometry*, 41(2):199–207, December 2008.

[Ope26] OpenAI. Ten advances in mathematics and theoretical computer science, August 2026. https://cdn.openai.com/pdf/ten-proofs-oai.pdf.