On Reduction Probability Models in Lattice Sieving

Marc Stevens, Michael Yonli

CWI, Cryptology Group, Amsterdam, The Netherlands

Abstract. In lattice sieving, the sphere model assumes that sieving elements are distributed close to or on a sphere with uniformly distributed direction. It is extensively used to predict how lattice sieving behaves. In the sphere model the probability that a random pair of vectors reduces is asymptotically $p_n = (3/4)^{n/2}/\sqrt{3\pi n/8}$. In practice sieving algorithms have been observed to perform better than predicted by the sphere model. It is an open question how this gap behaves asymptotically: does the gap vanish or grow as the dimension grows?
Our work answers this question by showing that it is *asymptotically constant*. We generalise the sphere model to uniform ball and non-uniform ball models and analyse reduction probability distributions. The reduction probability advantages of our models over the sphere model range from $\times 1.5$ up to $\times 8$.
Moreover, we examine scaled depth distributions (defined for dimension n as $w = -n \ln \|x\|$) in the asymptotic setting. Under global reductions the output scaled depth distribution converges to Exp(2/3) for any converging family of scaled depth distributions that is dominated by a suitable integrable function. The input scaled depth distribution only affects the total reduction probability. Compared to (the scaled depth distribution Exp(1) induced by) the uniform ball as input distribution, using this stable limit distribution as input distribution results in an increased reduction probability ($\times 4.5$ versus $\times 8$).

1 Introduction

Consider a lattice $\mathcal{L}$ and let λ_1 be the length of its shortest non-zero vector. Finding a vector $\boldsymbol{v} \in \mathcal{L} \setminus \{\mathbf{0}\}$ such that $\|\boldsymbol{v}\| = \lambda_1$ is known as the Shortest Vector Problem (SVP). Lattice sieving methods aim to solve SVP (or to find a sufficiently short vector) by maintaining a large list L of lattice elements, and repeatedly trying to find *reducing pairs*: i.e., $\boldsymbol{x}, \boldsymbol{y} \in L$ with distance $D(\boldsymbol{x}, \boldsymbol{y}) = \|\boldsymbol{x} - \boldsymbol{y}\|$ 'small', and then adding $\boldsymbol{x} - \boldsymbol{y}$ to the list (replacing either $\boldsymbol{x}, \boldsymbol{y}$, whichever is longer, or the longest element from the list).

In this work, we study models to analyse the probability that a pair reduces, as well as the distribution of the norms of the reductions found. Nguyen-Vidick [NV08] introduced the heuristic assumption that the list follows an isotropic distribution close to (or on) a sphere of radius r, that we refer to as the **sphere model**, and obtain an asymptotic expression for the reduction probability:

$$\Pr[\|\boldsymbol{x} - \boldsymbol{y}\| \leq r] \quad \sim \quad p_n \coloneqq \left(\tfrac{3}{4}\right)^{n/2} / \sqrt{3\pi n/8}.$$

Without loss of generality, we will use $r = 1$, i.e., the unit sphere as we can always rescale a lattice. An exact expression for the reduction probability uses the regularized incomplete beta function (e.g. [FBB+15]):

$$\Pr[\|\boldsymbol{x} - \boldsymbol{y}\| \leq 1] = \tfrac{1}{2} I_{3/4}(\tfrac{n-1}{2}, \tfrac{1}{2}). \tag{1}$$

The sphere model is used extensively throughout the lattice sieving literature, because of its simplicity and due to the fact that the mass of an n-dimensional ball concentrates at its boundary as $n \to \infty$. Indeed, this can be observed from the uniform distribution on the n-dimensional ball, which has length PDF $f(x) = nx^{n-1}$, that vanishes pointwise for any length $x < 1$ as $n \to \infty$.

However, in practice lattice sieving has been observed to perform better than expected given the sphere model, and it is an open question how this gap behaves asymptotically [AGPS20, ABD+21]. Does this gap vanish, or grow as the dimension grows? Our work answers this open question by presenting ball models and showing that the gap is *asymptotically constant*, with different constants for various cases.

Asymptotically, it seems that all radial information is lost from n-dimensional balls, and only the directional distribution is needed. However, analysing the **scaled depth** $w \coloneqq -n \ln x$, instead of lengths x, one finds that the distribution of the scaled depth is the exponential distribution Exp(1):

$$\Pr[w \geq \lambda] = \Pr[x \leq e^{-\lambda/n}] = \left(e^{-\lambda/n}\right)^n = e^{-\lambda}. \tag{2}$$

Note that the scaled depth maps normalized lengths $x \in (0, 1]$ to the unbounded interval $[0, \infty)$.This motivates us to look for better models that take the length distribution into account and to compare their advantage with the sphere model.

In this work we generalise the sphere model to the **ball model** and study both the uniform ball distribution and non-uniform ball distributions. For the uniform ball distribution, we derive equally simple asymptotic expressions for the reduction probability as for the sphere model. Non-uniform ball distributions enable the analysis of iterated sieving rounds: the output distribution of one round is the input distribution of the next, and we obtain results in terms of scaled depths. We find two cases where the output scaled depth distribution always tends to the exponential distribution Exp(2/3), for which we also derive asymptotic reduction probability expressions.

1.1 Contributions

We introduce a framework and tools to analyse the ball model for four slightly different sieving processes. We distinguish between two distance functions:

- *Fixed sign*: only $\|\boldsymbol{x} - \boldsymbol{y}\|$ is considered (or alternatively $\|\boldsymbol{x} + \boldsymbol{y}\|$):

$$D_{\text{-}}(\boldsymbol{x}, \boldsymbol{y}) \coloneqq \|\boldsymbol{x} - \boldsymbol{y}\| \quad \leq \|\boldsymbol{x}\| + \|\boldsymbol{y}\|$$

- *Optimised sign*: $\|\boldsymbol{x} - \boldsymbol{y}\|$ and $\|\boldsymbol{x} + \boldsymbol{y}\|$ are considered, using the shortest:

$$D_{\pm}(\boldsymbol{x}, \boldsymbol{y}) \coloneqq \min(\|\boldsymbol{x} - \boldsymbol{y}\|, \|\boldsymbol{x} + \boldsymbol{y}\|) \quad \leq \sqrt{\|\boldsymbol{x}\|^2 + \|\boldsymbol{y}\|^2}$$

But we also distinguish on the reduction criteria:

- *Local reductions*: $(\boldsymbol{x}, \boldsymbol{y})$ is a reducing pair $\Leftrightarrow D(\boldsymbol{x}, \boldsymbol{y}) \leq \max(\|\boldsymbol{x}\|, \|\boldsymbol{y}\|)$, when the longest of $\boldsymbol{x}$ and $\boldsymbol{y}$ is replaced by the shorter combination of $\boldsymbol{x}$ and $\boldsymbol{y}$.
- *Global reductions*: $(\boldsymbol{x}, \boldsymbol{y})$ reducing pair $\Leftrightarrow D(\boldsymbol{x}, \boldsymbol{y}) \leq \lambda$ for a global bound $\lambda \in \mathbb{R}_{>0}$, when the largest element of the list is replaced.

We label each of these four sieving cases using '`L-`', '`L±`', '`G-`', '`G±`'.

We first study the uniform ball model, a distribution that approximates the setting where lattice sieving is close to saturating a ball, i.e., it contains a significant fraction of all lattice elements shorter than a given radius. For the uniform ball model, we derive explicit output length distribution PDF and CDF formulae for any n and all four cases (in Section 3 and Lemma 3). From these, we obtain the following asymptotic result concerning the uniform ball model for these four cases:

Lemma 1. *Let X, Y be independently distributed uniformly on the n-dimensional unit ball, then asymptotically:*

$$\begin{aligned}
\Pr[D\text{-}(X,Y) \leq 1] &\sim 3\left(\tfrac{3}{4}\right)^{n/2}/\sqrt{2\pi n/3} &&= 2.25p_n \\
\Pr[D_{\pm}(X,Y) \leq 1] &\sim 6\left(\tfrac{3}{4}\right)^{n/2}/\sqrt{2\pi n/3} &&= 4.5p_n \\
\Pr[D\text{-}(X,Y) \leq \max(\|X\|,\|Y\|)] &\sim 2\left(\tfrac{3}{4}\right)^{n/2}/\sqrt{2\pi n/3} &&= 1.5p_n \\
\Pr[D_{\pm}(X,Y) \leq \max(\|X\|,\|Y\|)] &\sim 4\left(\tfrac{3}{4}\right)^{n/2}/\sqrt{2\pi n/3} &&= 3p_n
\end{aligned}$$

Corollary 1. *The above asymptotic reduction probabilities are larger by factors $(2.25, 4.5, 1.5, 3)$, respectively, compared to the sphere model. Hence, asymptotically the advantage of the uniform ball model is thus constant compared to the uniform sphere model, and does neither vanish, nor grow.*

We then study the non-uniform ball model, a more generic case for the lattice sieving setting where saturation is low. Non-uniform ball distributions enable the analysis of iterated sieving rounds: the output distribution of one round is the input distribution of the next. We first derive unified double integration expressions for all four cases in Section 4 and Lemma 5 and then develop the scaled depth framework and translate the unified double integration expressions to it in Section 5.

From these, we obtain asymptotic results concerning the asymptotic distributions of the scaled depth for the global reduction cases. For valid input distributions, we show that the output distribution is *independent* of the input distribution, and when used as input distribution itself results in higher reduction probabilities.

Lemma 2. *Let W_x, W_y represent the scaled depth of points X, Y of lengths $e^{-W_x/n}$, $e^{-W_y/n}$ on the n-dimensional unit ball, having independent identical isotropic distribution. Let $\{\widehat{f}_n\}_{n\geq 3}$ be a family of scaled depth distribution PDFs of W_x and W_y, where the index n corresponds to the dimension, converging to $\widehat{f}$*

Table 1. Overview of reduction probabilities and output distributions. Asymptotic results are denoted with $\sim$. Lemma 3 gives exact output distributions for the listed cases.

Case	Input distribution	Reduction probability	Output distribution
L-	$U(\mathcal{B}_n)$	$\sim 1.5 \cdot p_n$	Lemma 3
L±	$U(\mathcal{B}_n)$	$\sim 3 \cdot p_n$	Lemma 3
G-	$U(\mathcal{B}_n) = e^{-\operatorname{Exp}(1)/n}$	$\sim 2.25 \cdot p_n$	Lemma 3, $\sim e^{-\operatorname{Exp}(2/3)/n}$
G±	$U(\mathcal{B}_n) = e^{-\operatorname{Exp}(1)/n}$	$\sim 4.5 \cdot p_n$	Lemma 3, $\sim e^{-\operatorname{Exp}(2/3)/n}$
G-	$e^{-\operatorname{Exp}(2/3)/n}$	$\sim 4 \cdot p_n$	$\sim e^{-\operatorname{Exp}(2/3)/n}$
G±	$e^{-\operatorname{Exp}(2/3)/n}$	$\sim 8 \cdot p_n$	$\sim e^{-\operatorname{Exp}(2/3)/n}$
L-	$e^{-\operatorname{Exp}(2/3)/n}$	$\sim 2 \cdot p_n$	-
L±	$e^{-\operatorname{Exp}(2/3)/n}$	$\sim 4 \cdot p_n$	-

such that there exists an integrable v with $\widehat{f}_n(w) \le v(w)$ for all n and the integral $\int_0^\infty v(w)e^{w/3}\,\mathrm{d}w$ exists and is finite.

We define $W_\pm := -n \ln D_\pm(X,Y)$ and $W_- := -n \ln D_-(X,Y)$, the random variables of the output scaled depth for the two global reduction cases. Then asymptotically $W_\pm$ and W_- have exponential distribution $\operatorname{Exp}(2/3)$ *(after renormalization by the reduction probability).*

When $\widehat{f}(w) = ae^{-aw}$ corresponding to an exponential distribution $\operatorname{Exp}(a)$ *with $a > 1/3$ then the asymptotic reduction probabilities are:*

$$\Pr[D_-(X,Y) \le 1] = \Pr[W_- \ge 0] \;\sim\; \left(\tfrac{3a}{3a-1}\right)^2 \left(\tfrac{3}{4}\right)^{n/2} / \sqrt{3\pi n/8}$$
$$\Pr[D_\pm(X,Y) \le 1] = \Pr[W_\pm \ge 0] \;\sim\; 2\left(\tfrac{3a}{3a-1}\right)^2 \left(\tfrac{3}{4}\right)^{n/2} / \sqrt{3\pi n/8}$$

Corollary 2. *For* $\operatorname{Exp}(a)$*, the scaled depth distribution with $a = 1$ (uniform ball), the advantage over the sphere model is a factor* 2.25 *and* 4.5*, respectively, matching the previous corollary. For $a = 2/3$ (stable distribution) this is* 4 *and* 8*, respectively, a gain by a factor* $16/9 \approx 1.78$ *compared to $a = 1$.*

The proofs of Lemmas 1 and 2 are in Section 5, using the results in Sections 3 and 4, respectively.

1.2 Preliminaries

Let $\mathbb{R}^n$ be the n-dimensional Euclidean space, equipped with the canonical inner product $\langle \cdot, \cdot \rangle$ and norm $\|\boldsymbol{v}\| := \sqrt{\langle \boldsymbol{v}, \boldsymbol{v} \rangle}$ for $\boldsymbol{v} \in \mathbb{R}^n$. Let $\{\boldsymbol{e}_i\}_{1 \le i \le n}$ be the standard basis of $\mathbb{R}^n$. The i-th column vector of a matrix $\boldsymbol{A}$ will be denoted by $\boldsymbol{a}_i$, the i-th component of a vector $\boldsymbol{v}$ by v_i, and the i-th vector of the canonical basis of $\mathbb{R}^n$ by $\boldsymbol{e}_i$, where $i \in \{1, \ldots, n\}$. For non-zero $\boldsymbol{v}$, we write $\hat{\boldsymbol{v}} := \boldsymbol{v}/\|\boldsymbol{v}\|$. For non-zero $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^n$, their angle is denoted by $\angle(\boldsymbol{x}, \boldsymbol{y}) := \arccos(\langle \hat{\boldsymbol{x}}, \hat{\boldsymbol{y}} \rangle)$. The transpose of a matrix $\boldsymbol{A}$ is denoted by $\boldsymbol{A}^{\mathrm{T}}$. For $S \subset \mathbb{R}^n$, we define $S_* := S \setminus \{\boldsymbol{0}\}$.

Recall the definitions of the gamma function $\Gamma(z)$, the (incomplete) beta function $B(a,b)$ ($B_z(a,b)$) and the regularized incomplete beta function $I_z(a,b)$:

$$\Gamma(z) \coloneqq \int_0^\infty t^{z-1}e^{-t}\,\mathrm{d}t, \qquad B_z(a,b) \coloneqq \int_0^z t^{a-1}(1-t)^{b-1}\,\mathrm{d}t$$
$$B(a,b) \coloneqq B_1(a,b), \quad I_z(a,b) \coloneqq \tfrac{B_z(a,b)}{B(a,b)}, \quad I_{1-z}(a,b) = 1 - I_z(b,a)$$

Lattices. A lattice $\mathcal{L}$ is a discrete subgroup of $\mathbb{R}^n$ and every lattice admits a basis that generates it. For a matrix $\boldsymbol{B}$, we denote the lattice generated by $\boldsymbol{B}$ as $\mathcal{L}(\boldsymbol{B}) \coloneqq \{\boldsymbol{Bx} : \boldsymbol{x} \in \mathbb{Z}^n\}$. If $\boldsymbol{B}$ has full column rank and generates the lattice $\mathcal{L}$, then $\boldsymbol{B}$ is said to be a basis of $\mathcal{L}$. The Gram-Schmidt orthogonalization of a full rank matrix $\boldsymbol{B}$ is denoted by $\boldsymbol{B}^*$, with column vectors $\boldsymbol{b}_i^*$. The volume of a lattice $\mathrm{Vol}(\mathcal{L}(\boldsymbol{B})) \coloneqq \sqrt{\det(\boldsymbol{B}^\mathrm{T}\boldsymbol{B})} = \prod_i \|\boldsymbol{b}_i^*\|$ is independent of the choice of $\boldsymbol{B}$. The Gaussian heuristic [dv25] states that for a lattice $\mathcal{L}$ and a measurable $\mathcal{V} \subset \mathrm{span}(\mathcal{L})$,

$$|(\mathcal{L} \setminus \{\boldsymbol{0}\}) \cap \mathcal{V}| \approx \mathrm{Vol}(\mathcal{V}) / \mathrm{Vol}(\mathcal{L}). \tag{3}$$

Geometry. Let $\mathcal{B}_n \coloneqq \{\boldsymbol{v} \in \mathbb{R}^n : \|\boldsymbol{v}\| \leq 1\}$ be the n-dimensional unit ball centred at the origin, and $\mathcal{B}_n(\boldsymbol{c}, r) \coloneqq \boldsymbol{c} + r \cdot \mathcal{B}_n$ be the ball of radius r centred at $\boldsymbol{c}$. Their ($(n-1)$-dimensional) surfaces are the spheres $\mathcal{S}_{n-1}$ and $\mathcal{S}_{n-1}(\boldsymbol{c}, r)$, respectively. The volume of $r \cdot \mathcal{B}_n$ and area of $r \cdot \mathcal{S}_{n-1}$ are:

$$\mathrm{Vol}(r \cdot \mathcal{B}_n) = r^n \pi^{\frac{n}{2}} / \Gamma(1 + \tfrac{n}{2}) \quad \text{and} \quad \mathrm{Area}(r \cdot \mathcal{S}_{n-1}) = n r^{n-1} \pi^{\frac{n}{2}} / \Gamma(1 + \tfrac{n}{2})$$

For $z \in [-1, 1]$, we define the spherical cap $\mathcal{C}_{n-1}(z) \coloneqq \{\boldsymbol{v} \in \mathcal{S}_{n-1} : \langle \boldsymbol{v}, \boldsymbol{e}_1 \rangle \geq z\}$, and the ball cap $\mathcal{K}_n(z) \coloneqq \{\boldsymbol{v} \in \mathcal{B}_n : \langle \boldsymbol{v}, \boldsymbol{e}_1 \rangle \geq z\}$. Note that these differ from the usual definition using a height parameter $h \in [0, 2]$. The area of the spherical cap $r \cdot \mathcal{C}_{n-1}(z)$ is (cf. [Li10]):

$$\mathrm{Area}(r \cdot \mathcal{C}_{n-1}(z)) = \begin{cases} \mathrm{Area}(r \cdot \mathcal{S}_{n-1}) \cdot \frac{1}{2} I_{1-z^2}\left(\frac{n-1}{2}, \frac{1}{2}\right) & z \in [0, 1] \\ \mathrm{Area}(r \cdot \mathcal{S}_{n-1}) \cdot I_{\frac{1}{2}(1-z)}\left(\frac{n-1}{2}, \frac{n-1}{2}\right) & z \in [-1, 1] \end{cases} \tag{4}$$

Similarly, the volume of the ball cap $r \cdot \mathcal{K}_n(z)$ is (cf. [Li10]):

$$\mathrm{Vol}(r \cdot \mathcal{K}_n(z)) = \begin{cases} \mathrm{Vol}(r \cdot \mathcal{B}_n) \cdot \frac{1}{2} I_{1-z^2}\left(\frac{n+1}{2}, \frac{1}{2}\right) & z \in [0, 1] \\ \mathrm{Vol}(r \cdot \mathcal{B}_n) \cdot I_{\frac{1}{2}(1-z)}\left(\frac{n+1}{2}, \frac{n+1}{2}\right) & z \in [-1, 1] \end{cases} \tag{5}$$

Note that the two cases in Eq. (4) and Eq. (5) agree on $[0, 1]$ using [DLMF, §8.17(i).6], the extension to $[-1, 0]$ can be mapped to $[0, 1]$ using $I_{1-x}(a, a) = 1 - I_x(a, a)$.

Probability distributions. We denote a random variable X following a distribution $\mathcal{D}$ as $X \sim \mathcal{D}$. For two random variables X and Y, we write $X \sim Y$

if they have identical distributions. Sampling is denoted as $x \leftarrow X$ or $x \leftarrow \mathcal{D}$. For a function $f : \mathbb{R} \to \mathbb{R}$, we denote by $f(X)$ the random variable implied by the distribution of sampling $x \leftarrow X$ and outputting $f(x)$. For multivariate functions, we define $f(X_1, X_2, \ldots)$ analogously. The discrete (or continuous) uniform distribution on a finite set (or bounded volume) V is denoted by $U(V)$. For a continuous random variable X, let $F_X(x) = \Pr[X \leq x]$ and $f_X = F'_X$ (also denoted as $f_X(x)\,\mathrm{d}x = \Pr[X \in (x, x + \mathrm{d}x)]$) be the cumulative distribution function (CDF) and probability density function (PDF) of X, respectively. A CDF or PDF is called conditional when it is not normalized due to the underlying probability space being filtered, e.g., on that a pair reduces.

For $X = (X_1, \ldots, X_n) \sim U(\mathcal{S}_{n-1})$, each coordinate X_i has the following distributions:

$$\begin{aligned} F_{X_i}(z) &= 1 - \Pr[X_i \geq z] = 1 - \operatorname{Area}(\mathcal{C}_{n-1}(z))/\operatorname{Area}(\mathcal{S}_{n-1}) \qquad \text{for } z \in [-1, 1] \\ &= 1 - I_{(1-z)/2}\left(\tfrac{n-1}{2}, \tfrac{n-1}{2}\right) = I_{(z+1)/2}\left(\tfrac{n-1}{2}, \tfrac{n-1}{2}\right), \end{aligned} \tag{6}$$

$$\begin{aligned} F_{|X_i|}(z) &= 1 - 2\Pr[X_i \geq z] = 1 - 2\operatorname{Area}(\mathcal{C}_{n-1}(z))/\operatorname{Area}(\mathcal{S}_{n-1}) \qquad \text{for } z \in [0, 1] \\ &= 1 - I_{1-z^2}\left(\tfrac{n-1}{2}, \tfrac{1}{2}\right) = I_{z^2}\left(\tfrac{1}{2}, \tfrac{n-1}{2}\right). \end{aligned} \tag{7}$$

2 Lattice Sieving

We study reduction models of lattice sieving under the Gaussian heuristic. The Gaussian heuristic implies that the distribution of lattice elements is isotropic (i.e. the distribution has no directional bias), since it estimates the number of contained lattice elements purely based on volume.

More precisely, we assume that points are distributed according to a unit ball distribution $\mathcal{D} \sim \mathcal{R} \cdot U(\mathcal{S}_{n-1})$, where $U(\mathcal{S}_{n-1})$ represents the uniform directional component and $\mathcal{R}$ the radial or length component of the ball distribution. To model lattice sieving, we thus assume that a pair X, Y has been sampled according to $\mathcal{D}$. We study the distribution of the output reduction length: $D_{\text{-}}(X, Y)$ or $D_{\pm}(X, Y)$. We present methods that allow us to calculate these from $\mathcal{D}$.

We consider 4 different cases of lattice sieving described by the following (conditional) CDFs $F^{*}_{\mathcal{D}}(z)$:

$$\begin{aligned} F^{\mathtt{G}^{-}}_{\mathcal{D}}(z) &= \Pr[D_{\text{-}}(X, Y) \leq z : X, Y \sim \mathcal{D}] \\ F^{\mathtt{G}^{\pm}}_{\mathcal{D}}(z) &= \Pr[D_{\pm}(X, Y) \leq z : X, Y \sim \mathcal{D}] \\ F^{\mathtt{L}^{-}}_{\mathcal{D}}(z) &= \Pr[D_{\text{-}}(X, Y) \leq \min(z, \max(\|X\|, \|Y\|)) : X, Y \sim \mathcal{D}] \\ F^{\mathtt{L}^{\pm}}_{\mathcal{D}}(z) &= \Pr[D_{\pm}(X, Y) \leq \min(z, \max(\|X\|, \|Y\|)) : X, Y \sim \mathcal{D}] \end{aligned}$$

In each case we also derive the corresponding (conditional) PDFs $f^{*}_{\mathcal{D}}(z)$. Note that we also often refer to distributions by their PDFs f. For convenience, we also use '$\mathtt{ball}, n$' for the uniform ball distribution $F_{\mathtt{ball},n}(z) \coloneqq z^n$, and use '$\mathtt{sphere}, n$' for the uniform sphere distribution, which we treat as a discrete length distribution: $F_{\mathtt{sphere},n}(z) \coloneqq \mathbb{1}_{z \geq 1}$.

2.1 The sphere model

The sphere model assumes that elements of L (the list of elements maintained by a sieving algorithm) lie on $\mathcal{S}_{n-1}$, a simplification supported by the fact that the mass of a n-dimensional ball $\mathcal{B}_n$ concentrates near $\mathcal{S}_{n-1}$ as $n \to \infty$.

Note that there is no distinction between local and global reductions in the sphere model, since the criteria are equivalent when $\|X\| = \|Y\| = 1$. Therefore, we only examine the distance functions $(D_{\texttt{-}}, D_{\texttt{±}})$.

First, we show how to derive the reduction probability in the sphere model. For $X, Y \sim U(\mathcal{S}_{n-1})$, we can always apply a rotation Φ_X such that $\Phi_X(X) = \boldsymbol{e}_1$ and for any $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^n$ we have $\|\boldsymbol{x} - \boldsymbol{y}\| = \|\Phi_X(\boldsymbol{x}) - \Phi_X(\boldsymbol{y})\|$. As Y is isotropic and independent of X, we know $\Phi_X(Y) \sim U(\mathcal{S}_{n-1})$. Hence,

$$\|X - Y\| \quad \sim \quad \|\boldsymbol{e_1} - Y\| = \sqrt{\|\boldsymbol{e}_1\|^2 + \|Y\|^2 - 2\langle \boldsymbol{e}_1, Y\rangle} = \sqrt{2 - 2Y_1}.$$

Since the norm of $D_{\texttt{-}}(X, Y)$ is at most 2, it follows by Eq. (6) that:

$$\begin{aligned} F^{\texttt{G-}}_{\texttt{sphere},n}(z) &= \Pr[D_{\texttt{-}}(X, Y) \le z] = \Pr[Y_1 \ge 1 - z^2/2] \\ &= I_{z^2/4}(\tfrac{n-1}{2}, \tfrac{n-1}{2}), \quad z \in [0, 2], \\ f^{\texttt{G-}}_{\texttt{sphere},n}(z) &= \frac{z^{n-2}(1 - z^2/4)^{\frac{n-3}{2}}}{B(\frac{n-1}{2}, \frac{1}{2})} \end{aligned}$$

The distance function $D_{\texttt{±}}$ has a similar derivation using Eq. (7), except that $D_{\texttt{±}}(X, Y) \le \sqrt{2}$:

$$\begin{aligned} F^{\texttt{G±}}_{\texttt{sphere},n}(z) &= \Pr[D_{\texttt{±}}(X, Y) \le z] = \Pr[|Y_1| \ge 1 - z^2/2] \\ &= 2I_{z^2/4}(\tfrac{n-1}{2}, \tfrac{n-1}{2}) = 2F^{\texttt{G-}}_{\texttt{sphere},n}(z), \quad z \in [0, \sqrt{2}]. \\ f^{\texttt{G±}}_{\texttt{sphere},n}(z) &= 2f^{\texttt{G-}}_{\texttt{sphere},n}(z) \end{aligned}$$

This is exactly double the fixed-sign reduction probability, since both $X - Y$ and $X + Y$ are considered, without needing a correction term as they cannot both have norm less than $\sqrt{2}$.

3 Uniform Ball

In this section we first analyse the uniform ball case. Here, we assume $X, Y \sim U(\mathcal{B}_n)$, or equivalently $X, Y \sim \mathcal{R} \cdot U(\mathcal{S}_{n-1})$ with $\mathcal{R}$ defined by the CDF $F_{\texttt{ball},n}(x) = x^n$. We analyse each of the four reduction function+criteria cases below, and obtain the following results:

Lemma 3. *Consider the uniform unit ball distribution $\mathcal{D} \coloneqq U(\mathcal{B}_n)$ and the four output length distributions as defined in Section 2. The (conditional) CDFs*

$F^{\texttt{G-}}_{ball,n}(z)$, $F^{\texttt{G±}}_{ball,n}(z)$, $F^{\texttt{L-}}_{ball,n}(z)$, *and* $F^{\texttt{L±}}_{ball,n}(z)$ *are:*

label	$F^{label}_{ball,n}(z)$	$z \in$
`G-`	$z^n I_{1-z^2/4}(\frac{n+1}{2}, \frac{1}{2}) + I_{z^2/4}(\frac{n+1}{2}, \frac{n+1}{2})$	$[0, 2]$
`G±`	$2F^{\texttt{G-}}_{ball,n}(z) - \frac{z^{2n}}{2^n}(2F^{\texttt{G-}}_{ball,n}(2/z) - 1)$	$[0, \sqrt{2}]$
`L-`	$F^{\texttt{G-}}_{ball,n}(z) - \frac{1}{2} z^{2n} I_{3/4}(\frac{n+1}{2}, \frac{1}{2})$	$[0, 1]$
`L±`	$2F^{\texttt{L-}}_{ball,n}(z)$	$[0, 1]$

We define $F^{\texttt{G-}}_{ball,n}(z)$ *to be 0 for* $z < 0$ *and 1 for* $z > 2$*, and accordingly* $f^{\texttt{G-}}_{ball,n}(z) = 0$ *for* $z \notin [0, 2]$*. The four corresponding (conditional) PDFs are:*

label	$f^{label}_{ball,n}(z)$	$z \in$
`G-`	$n \cdot z^{n-1} \cdot I_{1-z^2/4}(\frac{n+1}{2}, \frac{1}{2})$	$[0, 2]$
`G±`	$2f^{\texttt{G-}}_{ball,n}(z) - \frac{nz^{2n-1}}{2^{n-1}}(2F^{\texttt{G-}}_{ball,n}(2/z) - 1) + \frac{z^{2n-2}}{2^{n-2}} f^{\texttt{G-}}_{ball,n}(2/z)$	$[0, \sqrt{2}]$
`L-`	$f^{\texttt{G-}}_{ball,n}(z) - nz^{2n-1} I_{3/4}(\frac{n+1}{2}, \frac{1}{2})$	$[0, 1]$
`L±`	$2f^{\texttt{L-}}_{ball,n}(z)$	$[0, 1]$

Note that $F^{\texttt{G-}}_{\texttt{ball},n}(2/z) = 1$ and $f^{\texttt{G-}}_{\texttt{ball},n}(2/z) = 0$ for $z \in [0, 1]$, hence the expressions for $F^{\texttt{G±}}_{\texttt{ball},n}(z)$ and $f^{\texttt{G±}}_{\texttt{ball},n}(z)$ simplify for $z \in [0, 1]$. The proofs for each case are written in Sections 3.2 to 3.5.

3.1 Odd dimension

The four explicit PDF and CDF expressions in Lemma 3 are polynomials over $\mathbb{Q}$ for odd dimension. Indeed, the incomplete beta expression in the PDFs (and CDFs) can be rewritten using [DLMF, §8.17(i).6] for $0 \le z \le 2$:

$$I_{1-z^2/4}(\tfrac{n+1}{2}, \tfrac{1}{2}) = 2I_{(2-z)/4}(\tfrac{n+1}{2}, \tfrac{n+1}{2}).$$

Then for odd n both parameters are integer and this results in an explicit polynomial expression:

$$I_x(m, k-m+1) = \sum_{j=m}^{k} \binom{k}{j} x^j (1-x)^{k-j}, \quad \text{for } k, m \in \mathbb{N} \text{ [DLMF, §8.17(i).5]} \quad (8)$$

We show example PDF polynomial expressions for low odd dimension in Table 2.

3.2 Proof for the global-reduction fixed-sign case

The global-reduction fixed-sign case is simply the output distribution $D_{\texttt{-}}(X, Y) = \|X - Y\|$ for $X, Y \sim U(\mathcal{B}_n)$, which has been studied before [KM63, p. 53–54]:

Lemma 4 (§2.48[KM63]). *The distribution of* $\|X - Y\| \in [0, 2]$ *for* $X, Y \sim U(\mathcal{B}_n)$ *is:*

$$\Pr[z < \|X - Y\| < z + \mathrm{d}z] = P_n(z)\,\mathrm{d}z, \quad P_n(z) \coloneqq n \cdot z^{n-1} \cdot I_{1-z^2/4}(\tfrac{n+1}{2}, \tfrac{1}{2})$$

Table 2. Example odd dimension polynomial expressions of $f^{label}_{\texttt{ball},n}(z)$ on $z \in [0,1]$.

`label`	$f^{\text{label}}_{\texttt{ball},3}(z)$	$f^{\text{label}}_{\texttt{ball},5}(z)$
`G-`	$3z^2 - \frac{9}{4}z^3 + \frac{3}{16}z^5$	$5z^4 - \frac{75}{16}z^5 + \frac{25}{32}z^7 - \frac{15}{256}z^9$
`G±`	$6z^2 - \frac{9}{2}z^3 - \frac{3}{8}z^5$	$10z^4 - \frac{75}{8}z^5 + \frac{25}{16}z^7 - \frac{55}{128}z^9$
`L-`	$3z^2 - \frac{9}{4}z^3 - \frac{3}{4}z^5$	$5z^4 - \frac{75}{16}z^5 + \frac{25}{32}z^7 - \frac{35}{32}z^9$
`L±`	$6z^2 - \frac{9}{2}z^3 - \frac{3}{2}z^5$	$10z^4 - \frac{75}{8}z^5 + \frac{25}{16}z^7 - \frac{35}{16}z^9$

Proof. Here is an alternative proof, with some slight abuse of notation. Let $V \coloneqq X - Y$, then we first look at the density of V at $\boldsymbol{v} \in \mathbb{R}^n$ (with $z = \|\boldsymbol{v}\|$), where we write $\boldsymbol{v} < V < \boldsymbol{v} + \mathrm{d}\boldsymbol{v}$ for the combined statement $\boldsymbol{v}_i < V_i < \boldsymbol{v}_i + \mathrm{d}\boldsymbol{v}_i$, i.e., that V is in the infinitesimal box of volume $\mathrm{d}\boldsymbol{v} = \mathrm{d}\boldsymbol{v}_1 \cdots \mathrm{d}\boldsymbol{v}_n$ at the point $\boldsymbol{v}$. We can express this density in terms of the volume of the intersection of two balls at distance z, which corresponds to two equal ball caps:

$$\begin{aligned}
&\Pr[\boldsymbol{v} < V < \boldsymbol{v} + \mathrm{d}\boldsymbol{v}] = \Pr[Y + \boldsymbol{v} < X < Y + \boldsymbol{v} + \mathrm{d}\boldsymbol{v}] \\
&= \Pr[Y + \boldsymbol{v} \in \mathcal{B}_n] \Pr[Y + \boldsymbol{v} < X < Y + \boldsymbol{v} + \mathrm{d}\boldsymbol{v} : Y + \boldsymbol{v} \in \mathcal{B}_n] \\
&= \frac{\mathrm{Vol}(\mathcal{B}_n \cap (\boldsymbol{v} + \mathcal{B}_n))}{\mathrm{Vol}(\mathcal{B}_n)} \frac{\mathrm{d}\boldsymbol{v}}{\mathrm{Vol}(\mathcal{B}_n)} = \frac{2\,\mathrm{Vol}(\mathcal{K}_n(z/2))}{\mathrm{Vol}(\mathcal{B}_n)} \frac{\mathrm{d}\boldsymbol{v}}{\mathrm{Vol}(\mathcal{B}_n)} \\
&= I_{1-z^2/4}(\tfrac{n+1}{2}, \tfrac{1}{2}) \frac{\mathrm{d}\boldsymbol{v}}{\mathrm{Vol}(\mathcal{B}_n)}
\end{aligned}$$

Note that the density at $\boldsymbol{v}$ only depends on $\|\boldsymbol{v}\|$. We analyse $\|V\|$ by combining how many infinitesimal $\mathrm{d}\boldsymbol{v}$-sized disjoint boxes fit in the shell of radius z and thickness $\mathrm{d}z$, and the common density for each $\mathrm{d}\boldsymbol{v}$-sized box at radius z:

$$\begin{aligned}
&\Pr[z < \|v\| < z + \mathrm{d}z] = \Pr[z\boldsymbol{e}_1 < V < z\boldsymbol{e}_1 + \mathrm{d}\boldsymbol{v}] \cdot \frac{\mathrm{Vol}((z + \mathrm{d}z) \cdot \mathcal{B}_n \setminus z \cdot \mathcal{B}_n)}{\mathrm{d}\boldsymbol{v}} \\
&= I_{1-z^2/4}(\tfrac{n+1}{2}, \tfrac{1}{2}) \cdot \frac{\mathrm{d}\boldsymbol{v} \cdot (nz^{n-1}\,\mathrm{d}z) \cdot \mathrm{Vol}(\mathcal{B}_n)}{\mathrm{Vol}(\mathcal{B}_n) \cdot \mathrm{d}\boldsymbol{v}} = n \cdot z^{n-1} \cdot I_{1-z^2/4}(\tfrac{n+1}{2}, \tfrac{1}{2})\,\mathrm{d}z.
\end{aligned}$$

□

We now state the proof for the CDF $F^{\texttt{G-}}_{\texttt{ball},n}$ and PDF $f^{\texttt{G-}}_{\texttt{ball},n}$ from Lemma 3:

Proof. The PDF is simply $P_n(z)$ by definition. We derive the CDF $\int_0^z P_n(t)\,\mathrm{d}t$ using integration by parts with

$$u \coloneqq I_{1-t^2/4}(a,b),\ a \coloneqq \tfrac{n+1}{2}, b \coloneqq \tfrac{1}{2} \qquad dv \coloneqq nt^{n-1}\,\mathrm{d}t \quad \Rightarrow \quad v = t^n.$$

The derivative of u using the definition of $I_x(a,b)$ is:

$$\frac{\mathrm{d}}{\mathrm{d}t} I_{1-t^2/4}(a,b) = \frac{(1-t^2/4)^{a-1} \cdot (t^2/4)^{-1/2}}{B(a,b)} \cdot \frac{-t}{2} = -\frac{(1-t^2/4)^{a-1}}{B(a,b)}.$$

Integration by parts gives $\int_0^z u\,\mathrm{d}v = [vu]_0^z - \int_0^z v\,\mathrm{d}u$:

$$\int_0^z P_n(t)\,\mathrm{d}t = \left[t^n I_{1-t^2/4}(a,b)\right]_0^z + \int_0^z t^n \frac{(1-t^2/4)^{a-1}}{B(a,b)}\,\mathrm{d}t,$$
$$\int_0^z P_n(t)\,\mathrm{d}t = z^n I_{1-z^2/4}(a,b) + \frac{1}{B(a,b)} J(z), \quad J(z) \coloneqq \int_0^z t^n (1-t^2/4)^{(n-1)/2}\,\mathrm{d}t.$$

Substituting $r = t/2$ in $J(z)$'s integral, we obtain (using $\mathrm{d}t = 2\,\mathrm{d}r$):

$$J(z) = \int_0^{z/2} (2r)^n (1-r^2)^{(n-1)/2} 2\,\mathrm{d}r = 2^{n+1} \int_0^{z/2} r^n (1-r^2)^{(n-1)/2}\,\mathrm{d}r.$$

Then substituting $s = r^2$ (using $2r\,\mathrm{d}r = \mathrm{d}s$):

$$J(z) = 2^n \int_0^{z^2/4} s^{(n-1)/2}(1-s)^{(n-1)/2}\,\mathrm{d}s = 2^n B(\tfrac{n+1}{2}, \tfrac{n+1}{2}) I_{z^2/4}(\tfrac{n+1}{2}, \tfrac{n+1}{2}).$$

Finally, we get the desired result if $2^n B(\frac{n+1}{2}, \frac{n+1}{2})/B(\frac{n+1}{2}, \frac{1}{2}) = 1$. This can be proven by expanding $B(a,b) = \Gamma(a)\Gamma(b)/\Gamma(a+b)$:

$$\frac{2^n B(\frac{n+1}{2}, \frac{n+1}{2})}{B(\frac{n+1}{2}, \frac{1}{2})} = \frac{2^n \Gamma(\frac{n+1}{2})^2 \Gamma(\frac{n+2}{2})}{\Gamma(n+1)\Gamma(\frac{n+1}{2})\Gamma(\frac{1}{2})} = \frac{2^n \Gamma(\frac{n+1}{2})\Gamma(\frac{n+2}{2})}{\sqrt{\pi}\Gamma(n+1)}.$$

The deduplication formula [DLMF, §5.5(iii).5] gives $\sqrt{\pi}\Gamma(2x) = 2^{2x-1}\Gamma(x)\Gamma(x+\frac{1}{2})$, which using $x = \frac{n+1}{2}$ makes the above fraction equal to 1. □

3.3 Proof for the global-reduction optimised-sign case

Proof. The PDF $f^{\mathtt{G\pm}}_{\mathtt{ball},n}(z)$ follows from differentiating the CDF using the chain rule. The CDF $F^{\mathtt{G\pm}}_{\mathtt{ball},n}(z)$ can be derived from the global-reduction fixed-sign result, exploiting the symmetry $Y \sim -Y$ with a correction term. We can rewrite the CDF using inclusion-exclusion as follows:

$$\begin{aligned}
F^{\mathtt{G\pm}}_{\mathtt{ball},n}(z) &= \Pr[\min(\|X-Y\|, \|X+Y\|) \le z] \\
&= \Pr[\|X-Y\| \le z] + \Pr[\|X+Y\| \le z] \\
&\quad - \Pr[\|X-Y\| \le z \wedge \|X+Y\| \le z] \\
&= 2F^{\mathtt{G-}}_{\mathtt{ball},n}(z) - \Pr[\|X-Y\| \le z \wedge \|X+Y\| \le z]
\end{aligned}$$

Since we use the uniform ball distribution, we can relate that last probability to the ratio between the volume of the region of valid $(X,Y) \in \mathcal{B}_n^2$ and the volume of the unit ball squared ($V_n \coloneqq \mathrm{Vol}(\mathcal{B}_n)$):

$$Q_n(z) \coloneqq \Pr[\|X-Y\| \le z \wedge \|X+Y\| \le z] = \frac{\mathrm{Vol}(\{(X,Y) : \max(\|X-Y\|, \|X+Y\|) \le z\})}{V_n^2}.$$

We apply the following transformation T on $\mathbb{R}^{2n}$:

$$T : (X,Y) \to (U,V) = \left(\tfrac{X+Y}{\sqrt{2}}, \tfrac{X-Y}{\sqrt{2}}\right), \quad X = \tfrac{U+V}{\sqrt{2}}, Y = \tfrac{U-V}{\sqrt{2}}.$$

This transformation T is orthogonal as:

$$\|U\|^2+\|V\|^2 = (\|X\|^2+\|Y\|^2+2\langle X,Y\rangle+\|X\|^2+\|Y\|^2-2\langle X,Y\rangle)/2 = \|X\|^2+\|Y\|^2.$$

Define the following regions of $\mathbb{R}^{2n}$, where A is the region where $\max(\|X-Y\|, \|X+Y\|) \le z$ and B_-, B_+ the regions that $Y \notin \mathcal{B}_n$, $X \notin \mathcal{B}_n$ respectively:

$$A \coloneqq \{\max(\|U\|, \|V\|)\sqrt{2} \le z\}, B_- \coloneqq \{\|U-V\| > \sqrt{2}\}, B_+ \coloneqq \{\|U+V\| > \sqrt{2}\}.$$

Then we rewrite Q_n using inclusion-exclusion:

$$Q_n(z)V_n^2 = \mathrm{Vol}(A) - \mathrm{Vol}(A \cap B_-) - \mathrm{Vol}(A \cap B_+) + \mathrm{Vol}(A \cap B_- \cap B_+).$$

Note that by symmetry of X and Y we have $\mathrm{Vol}(A \cap B_-) = \mathrm{Vol}(A \cap B_+)$, and that $\mathrm{Vol}(A \cap B_- \cap B_+) = 0$ due to the following contradiction:

$$4 < \|U+V\|^2 + \|U-V\|^2 = 2\|U\|^2 + 2\|V\|^2 \le 2z^2 \le 4.$$

Since A corresponds to the product of two balls of radius $\frac{z}{\sqrt{2}}$:

$$\begin{aligned}
\mathrm{Vol}(A) &= \mathrm{Vol}(\tfrac{z}{\sqrt{2}}\mathcal{B}_n^2) = 2^{-n}z^{2n}V_n^2, \\
\mathrm{Vol}(A \cap B_-) &= \mathrm{Vol}(A) \cdot \Pr[\|U-V\| > \sqrt{2} : U, V \sim U(\tfrac{z}{\sqrt{2}}\mathcal{B}_n)] \\
&= 2^{-n}z^{2n}V_n^2 \Pr[\|U'-V'\| > \tfrac{2}{z} : U', V' \sim U(\mathcal{B}_n)] \\
&= 2^{-n}z^{2n}V_n^2 \cdot \begin{cases} 0 & 0 \le z \le 1 \\ 1 - F^{\mathtt{G-}}_{\mathtt{ball},n}(\frac{2}{z}) & 1 \le z \le \sqrt{2}, \end{cases}.
\end{aligned}$$

Now $F^{\mathtt{G\pm}}_{\mathtt{ball},n}$ appears by collecting all terms for $z \le 1$ and for $z \ge 1$. □

3.4 Proof for the local-reduction fixed-sign case

Proof. We can also extend the results for the global-reduction fixed-sign case to the local-reduction fixed-sign case. We prove the result for the conditional CDF $F^{\mathtt{L-}}_{\mathtt{ball},n}$ (it is not normalized due to the local filtering), after which the PDF $f^{\mathtt{L-}}_{\mathtt{ball},n}$ follows.

$$\begin{aligned}
F^{\mathtt{L-}}_{\mathtt{ball},n}(z) &= \Pr[\|X-Y\| \le z \wedge \|X-Y\| \le \max(\|X\|, \|Y\|)] \\
&= \Pr[\|X-Y\| \le z < \max(\|X\|, \|Y\|)] \quad \text{(case A)} \\
&\quad + \Pr[\|X-Y\| \le \max(\|X\|, \|Y\|) \le z] \quad \text{(case B)}
\end{aligned}$$

We can rewrite case A as:

$$\begin{aligned}
&\Pr[\|X-Y\| \le z < \max(\|X\|, \|Y\|)] \\
=&\Pr[\|X-Y\| \le z] - \Pr[\|X-Y\| \le z \wedge \|X\|, \|Y\| \le z] \\
=&F^{\mathtt{G-}}_{\mathtt{ball},n}(z) - \Pr[\|X-Y\| \le z : \|X\|, \|Y\| \le z] \cdot \Pr[\|X\|, \|Y\| \le z] \\
=&F^{\mathtt{G-}}_{\mathtt{ball},n}(z) - F^{\mathtt{G-}}_{\mathtt{ball},n}(1) \cdot z^{2n} = F^{\mathtt{G-}}_{\mathtt{ball},n}(z) - \tfrac{3}{2}z^{2n}I_{3/4}(\tfrac{n+1}{2}, \tfrac{1}{2})
\end{aligned}$$

For the last step we use that X, Y conditioned on $\|X\|, \|Y\| \leq z$ are distributed as $X, Y \sim U(z \cdot \mathcal{B}_n)$. By rescaling we obtain $\Pr[\|X - Y\| \leq 1] = F^{\texttt{G-}}_{\texttt{ball},n}(1)$.

For case B we can also first rescale z to 1, assume without loss of generality that $\|X\| = \max(\|X\|, \|Y\|)$, and rescale X to the unit sphere:

$$\begin{aligned}
&\Pr[\|X - Y\| \leq \max(\|X\|, \|Y\|) \leq z] \\
=&\Pr[\|X\|, \|Y\| \leq z] \cdot \Pr[\|X - Y\| \leq \max(\|X\|, \|Y\|) : \|X\|, \|Y\| \leq z] \\
=&z^{2n} \cdot \Pr[\|X - Y\| \leq \max(\|X\|, \|Y\|)] \qquad \text{(rescale by } 1/z) \\
=&z^{2n} \cdot \Pr[\|X - Y\| \leq 1 : X \sim U(\mathcal{S}_{n-1}), Y \sim U(\mathcal{B}_n)] \quad \text{(rescale by } 1/\|X\|) \\
=&z^{2n} \cdot \Pr[\|\boldsymbol{e}_1 - Y\| \leq 1 : X = \boldsymbol{e}_1, Y \sim U(\mathcal{B}_n)] \quad \text{(rotate s/t } X = \boldsymbol{e}_1) \\
=&z^{2n} \cdot \frac{\mathrm{Vol}(\mathcal{B}_n \cap (\boldsymbol{e}_1 + \mathcal{B}_n))}{\mathrm{Vol}(\mathcal{B}_n)} = z^{2n} \cdot \frac{2\,\mathrm{Vol}(\mathcal{K}_n(\frac{1}{2}))}{\mathrm{Vol}(\mathcal{B}_n)} \\
=&z^{2n} \cdot I_{3/4}(\tfrac{n+1}{2}, \tfrac{1}{2}).
\end{aligned}$$

Here, we used that the intersection of two unit balls at distance 1 is the union of two ball caps cut out by the plane exactly midway between the two balls. □

3.5 Proof for the local-reduction optimised-sign case

Proof. This case follows easily from the local-reduction fixed-sign case. We prove the result for the conditional CDF $F^{\texttt{L±}}_{\texttt{ball},n}$, after which the conditional PDF $f^{\texttt{L±}}_{\texttt{ball},n}$ follows.

$$\begin{aligned}
F^{\texttt{L±}}_{\texttt{ball},n}(z) =& \Pr[D_{\pm}(X, Y) \leq \min(z, \max(\|X\|, \|Y\|))] \\
=& \Pr[\|X - Y\| \leq \min(z, \max(\|X\|, \|Y\|))] \\
&+ \Pr[\|X + Y\| \leq \min(z, \max(\|X\|, \|Y\|))] \\
&- \Pr[\max(\|X - Y\|, \|X + Y\|) \leq \min(z, \max(\|X\|, \|Y\|))] \\
=& F^{\texttt{L-}}_{\texttt{ball},n}(z) + F^{\texttt{L-}}_{\texttt{ball},n}(z) + 0.
\end{aligned}$$

Here, we use inclusion-exclusion, and since $-Y$ has the same distribution as Y:

$$\Pr[\|X+Y\| \leq \min(z, \max(\|X\|, \|Y\|))] = \Pr[\|X-Y\| \leq \min(z, \max(\|X\|, \|Y\|))]$$

Finally, the third term has probability 0, because $\|X - Y\|$ and $\|X + Y\|$ cannot both be smaller than $\|X\|$ (and $\|Y\|$ as well). □

4 The Non-Uniform Ball Model

We generalise the ball model analysis from the uniform distribution to non-uniform distributions, which requires a more general approach. This also enables us to consider iterated sieving distributions, where an output distribution is used as an input distribution in a next round.

Assume an isotropic distribution over the unit ball $\mathcal{B}_n$ with a given (non-uniform) length distribution. More specifically, we model $X, Y \sim \mathcal{D} = \mathcal{R} \cdot U(\mathcal{S}_{n-1})$ with a distribution split into a uniformly distributed direction component $U(\mathcal{S}_{n-1})$ and a length distribution $\mathcal{R}$ over $[0, 1]$. E.g., the uniform ball distribution has length distribution with CDF $F_{\texttt{ball},n}(x) = \mathrm{Vol}(x \cdot \mathcal{B}_n)/\mathrm{Vol}(\mathcal{B}_n) = x^n$ and PDF $f_{\texttt{ball},n}(x) = n \cdot x^{n-1}$.

Lemma 5. *Given an isotropic distribution $\mathcal{D}$ over $\mathcal{B}_n$ with length PDF $f(x)$, the output distributions for each of the four defined cases $\star \in \{\texttt{G-}, \texttt{G±}, \texttt{L-}, \texttt{L±}\}$ are:*

$$f^{\star}_{\mathcal{D}}(z) = c_{\star} \iint_{R_{\star}(z)} f(x) f(y) E_n(x, y, z)\, \mathrm{d}x\, \mathrm{d}y, \quad \textit{where}$$

$$E_n(x, y, z) \coloneqq \frac{z}{xy} \frac{\left(1 - g(x, y, z)^2\right)^{(n-3)/2}}{B(\frac{n-1}{2}, \frac{1}{2})}, \quad g(x, y, z) \coloneqq \frac{x^2 + y^2 - z^2}{2xy}$$

The constant $c_{\star}$ and integration region $R_{\star}(z)$ depend on the case:

$\star$	$c_{\star}$	$R_{\star}(z)$
G-	1	$\{(x, y) \in [0, 1]^2 \ : \ -1 < g(x, y, z) < 1\}$
G±	2	$\{(x, y) \in [0, 1]^2 \ : \ 0 < g(x, y, z) < 1\}$
L-	1	$\{(x, y) \in [0, 1]^2 \ : \ -1 < g(x, y, z) < 1 \wedge \max(x, y) \geq z\}$
L±	2	$\{(x, y) \in [0, 1]^2 \ : \ 0 < g(x, y, z) < 1 \wedge \max(x, y) \geq z\}$

The proofs for theses cases are written in Sections 4.1 to 4.3.

Comparison between cases. In Fig. 1 we have plotted the four integration regions $R_{\texttt{G±}}$, $R_{\texttt{L±}}$, $R_{\texttt{G-}}$, and $R_{\texttt{L-}}$, note that

$$R_{\texttt{L-}}(z) = R_{\texttt{L±}}(z) \subset R_{\texttt{G±}} \subset R_{\texttt{G-}}.$$

Considering global reduction, the main difference between fixed-sign and sign-optimised is that fixed-sign also includes the region where $-1 < g(x, y, z) < 0$, which corresponds to $(x^2 + y^2 < z^2) \wedge (x + y > z)$. This extra region increases the reduction probability, but it is effectively where the 'smallest' x and/or y occur, which tend to have vanishing probability density as the dimension grows. Thus unfortunately, from our evaluations it is clear that the benefit of the extra region quickly vanishes as the dimension grows, while the factor $\frac{1}{2}$ difference compared to the sign-optimised case is constant.

Considering local reduction, the local reduction regions are identical and are the 'smallest' integration regions of all four cases. This makes it clear that local reduction will always have a smaller reduction probability compared to global reduction, and that the reduction probability in the fixed-sign case is exactly a factor 2 less than for the sign-optimised case.

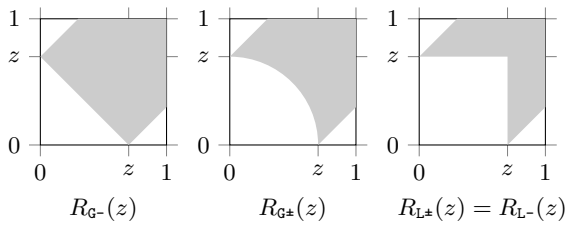

Fig. 1. Integration regions

4.1 Proof for global-reduction optimised-sign case

Given an input distribution $\mathcal{D}$ with length PDF $f(x)$, we can derive the output length distribution as follows. We first cover the 'global-reductions + sign-optimised' case, referred to by `G±`. Later, we describe how the other three cases (`G-`, `L±`, `L-`) can be handled.

Let $X, Y \sim \mathcal{D} = \mathcal{R} \cdot U(\mathcal{S}_{n-1})$, we will write $\boldsymbol{x} = x \cdot \boldsymbol{v}$ and $\boldsymbol{y} = y \cdot \boldsymbol{w}$, with $x, y \sim \mathcal{R}$ and $\boldsymbol{v}, \boldsymbol{w} \sim U(\mathcal{S}_{n-1})$. The PDF and CDF of the output distribution of $D_{\pm}(X, Y)$ are denoted as $f_{\mathcal{D}}^{\texttt{G±}}(z)$, $F_{\mathcal{D}}^{\texttt{G±}}(z)$, respectively. Using the same rotation trick explained for the sphere model, we can simply sample $\boldsymbol{x} = x \cdot \boldsymbol{e}_1$ and $\boldsymbol{y} = y \cdot \boldsymbol{w}$, where $x, y \sim \mathcal{R}$ and $\boldsymbol{w} \sim U(\mathcal{S}_{n-1})$. Then we can express the CDF $F_{\mathcal{D}}^{\texttt{G±}}(z)$ of the output length distribution as follows:

$$
\begin{aligned}
F_{\mathcal{D}}^{\texttt{G±}}(z) &= \Pr[D_{\pm}(X, Y) \leq z : X, Y \sim U(\mathcal{S}_{n-1}) \cdot \mathcal{D}] \\
&= \Pr[D_{\pm}(x \cdot \boldsymbol{e}_1, y \cdot \boldsymbol{w}) \leq z : x, y \sim \mathcal{D}, \boldsymbol{w} \sim U(\mathcal{S}_{n-1})] \\
&= \Pr[x^2 + y^2 - 2xy|w_1| \leq z^2 : x, y \sim \mathcal{D}, \boldsymbol{w} \sim U(\mathcal{S}_{n-1})] \\
&= \Pr\left[|w_1| \geq \frac{x^2 + y^2 - z^2}{2xy} : x, y \sim \mathcal{D}, \boldsymbol{w} \sim U(\mathcal{S}_{n-1})\right] \\
&= \int_0^1 \int_0^1 f(x) \cdot f(y) \cdot \Pr\left[|w_1| \geq g(x, y, z) : \boldsymbol{w} \sim U(\mathcal{S}_{n-1})\right] \mathrm{d}x \, \mathrm{d}y,
\end{aligned}
$$

where $g(x, y, z) \coloneqq (x^2 + y^2 - z^2)/(2xy)$ is as defined earlier for convenience. The internal probability expression on $|w_1|$ splits into three cases:

$$
\Pr\left[|w_1| \geq h : \boldsymbol{w} \leftarrow U(\mathcal{S}_{n-1})\right] = \begin{cases} 0 & \text{if } h \geq 1 \\ 1 & \text{if } h \leq 0 \\ I_{1-h^2}(\frac{n-1}{2}, \frac{1}{2}) & \text{if } 0 < h < 1 \end{cases} \tag{9}
$$

The above function is continuous and differentiable in h, except at $h = 0$ where it is continuous, but not differentiable. Since the only non-constant expression is for the $0 < h < 1$ case, one finds that the corresponding PDF of the output

length distribution is:

$$\begin{aligned}
f_{\mathcal{D}}^{\mathtt{G}\pm}(z) = \frac{\mathrm{d}F_{\mathcal{D}}^{\mathtt{G}\pm}(z)}{\mathrm{d}z} &= \int_0^1 \int_0^1 f(x)\cdot f(y)\cdot \left(\frac{\mathrm{d}}{\mathrm{d}z}\Pr\left[|w_1| \geq g(x,y,z)\right]\right) \mathrm{d}x\,\mathrm{d}y \\
&= \iint_{R_{\mathtt{G}\pm}(z)} f(x)\cdot f(y)\cdot \left(\frac{\mathrm{d}}{\mathrm{d}z} I_{1-g(x,y,z)^2}(\tfrac{n-1}{2},\tfrac{1}{2})\right) \mathrm{d}x\,\mathrm{d}y, \\
&= \iint_{R_{\mathtt{G}\pm}(z)} f(x)\cdot f(y)\cdot \left(\frac{2z}{xy}\frac{(1-g(x,y,z)^2)^{(n-3)/2}}{B(\frac{n-1}{2},\frac{1}{2})}\right) \mathrm{d}x\,\mathrm{d}y, \\
&= 2\iint_{R_{\mathtt{G}\pm}(z)} f(x)\cdot f(y)\cdot E_n(x,y,z)\,\mathrm{d}x\,\mathrm{d}y,
\end{aligned}$$

where $R_{\mathtt{G}\pm}(z) \coloneqq \{(x,y) \in [0,1]^2 : 0 < g(x,y,z) < 1\}$ represents the PDF integration region, i.e., the region where Eq. (9) is non-constant.

4.2 Proof for global-reduction fixed-sign case

Here, the derivation follows similarly to the optimised-sign case, except that the inner-probability statement is adjusted and no longer uses the absolute value of w_1:

$$\begin{aligned}
F_{\mathcal{D}}^{\mathtt{G}-}(z) &= \Pr[D_{\text{-}}(X,Y) \leq z : X,Y \sim U(\mathcal{S}_{n-1})\cdot\mathcal{D}] \\
&= \Pr[x^2+y^2-2xyw_1 \leq z^2 : x,y \sim \mathcal{R}, \boldsymbol{w} \sim U(\mathcal{S}_{n-1})] \\
&= \int_0^1\int_0^1 f(x)\cdot f(y)\cdot \Pr\left[w_1 \geq g(x,y,z) : \boldsymbol{w} \leftarrow U(\mathcal{S}_{n-1})\right]\,\mathrm{d}x\,\mathrm{d}y
\end{aligned}$$

The internal probability expression on w_1 also splits out into three cases:

$$\Pr\left[w_1 \geq h : \boldsymbol{w} \leftarrow U(\mathcal{S}_{n-1})\right] = \begin{cases} 0 & \text{if } h \geq 1 \\ 1 & \text{if } h \leq -1 \\ I_{(1-h)/2}(\frac{n-1}{2},\frac{n-1}{2}) & \text{if } -1 < h < 1 \end{cases}$$

The above function is everywhere continuous and differentiable in h. Since the only non-constant expression is for the $-1 < h < 1$ case, one finds that the corresponding PDF of the output length distribution is:

$$\begin{aligned}
f_{\mathcal{D}}^{\mathtt{G}-}(z) = \frac{\mathrm{d}F_{\mathcal{D}}^{\mathtt{G}-}(z)}{\mathrm{d}z} &= \int_0^1\int_0^1 f(x)\cdot f(y)\cdot\left(\frac{\mathrm{d}}{\mathrm{d}z}\Pr\left[w_1 \geq g(x,y,z)\right]\right)\mathrm{d}x\,\mathrm{d}y, \\
&= \iint_{R_{\mathtt{G}-}(z)} f(x)\cdot f(y)\cdot\left(\frac{d}{dz} I_{(1-g(x,y,z))/2}(\tfrac{n-1}{2},\tfrac{n-1}{2})\right)\mathrm{d}x\,\mathrm{d}y, \\
&= \iint_{R_{\mathtt{G}-}(z)} f(x)\cdot f(y)\cdot\left(\frac{2z}{xy}\frac{(1-g(x,y,z)^2)^{(n-3)/2}}{2^{n-1}B(\frac{n-1}{2},\frac{n-1}{2})}\right)\mathrm{d}x\,\mathrm{d}y, \\
&= \iint_{R_{\mathtt{G}-}(z)} f(x)\cdot f(y)\cdot E_n(x,y,z)\,\mathrm{d}x\,\mathrm{d}y,
\end{aligned}$$

where $R_{\texttt{G-}}(z) \coloneqq \{(x,y) \in [0,1]^2 : -1 < g(x,y,z) < 1\}$ represents the PDF integration region for the global-reduction + fixed-sign case. We used the fact that $B(\frac{n-1}{2}, \frac{1}{2}) = 2^{n-2}B(\frac{n-1}{2}, \frac{n-1}{2})$ (follows from [DLMF, 5.12.1+5.5.5]). Other than a factor 2 less and a change in integration region, the core expression is identical to the previous case.

4.3 Proof of local reduction cases

For the local reduction cases, the constraint $D(\boldsymbol{x}, \boldsymbol{y}) \le z$ is tightened to $D(\boldsymbol{x}, \boldsymbol{y}) \le \max(\|\boldsymbol{x}\|, \|\boldsymbol{y}\|)$. This implies that a pair $\boldsymbol{x}, \boldsymbol{y}$ with $D(\boldsymbol{x}, \boldsymbol{y}) \le z$ is only considered a reducing pair if $\max(\|\boldsymbol{x}\|, \|\boldsymbol{y}\|) \ge z$. Hence, the local reduction cases follow directly from the global reduction cases with a simple change of the integration regions.

5 Asymptotic analysis

5.1 Sphere Model

Let us first derive the more precise asymptotic expression p_n for the reduction probability in the sphere model $\Pr[\|\boldsymbol{x} - \boldsymbol{y}\| \le 1]$. We can derive a useful asymptotic expression for the incomplete beta $I_{3/4}(a, \frac{1}{2})$ that will reappear several times in this section; it follows from repeatedly applying a recursive relation [DLMF, §8.17(iv).18] and Stirling's approximation:

$$\begin{aligned} I_{3/4}(a, \tfrac{1}{2}) = \frac{B_{3/4}(a, \frac{1}{2})}{B(a, \frac{1}{2})} &\sim \frac{\frac{2(3/4)^a}{a} - \frac{3(3/4)^a}{a(a+1)} + \frac{27(3/4)^a}{2a(a+1)(a+2)} + \dots}{\sqrt{\pi/a}} \\ &\sim \frac{\frac{2}{a}(3/4)^a(1 - O(a^{-1}))}{\sqrt{\pi/a}} \sim \tfrac{2}{\sqrt{\pi a}} \left(\tfrac{3}{4}\right)^a (1 + O(a^{-1})) \sim \left(\tfrac{3}{4}\right)^a \tfrac{2}{\sqrt{\pi a}} \end{aligned} \tag{10}$$

Moreover, we have $I_{3/4}(a, \frac{1}{2}) = 2I_{1/4}(a, a)$ using [DLMF, §8.17(i).6] at $z = 1$.

The sphere model's reduction probability (see Section 2.1) is:

$$F^{\texttt{G-}}_{\texttt{sphere},n}(1) = I_{1/4}(\tfrac{n-1}{2}, \tfrac{n-1}{2}) = \tfrac{1}{2} I_{3/4}(\tfrac{n-1}{2}, \tfrac{1}{2}),$$

we use Eq. (10) with $a = \frac{n-1}{2}$ and obtain:

$$F^{\texttt{G-}}_{\texttt{sphere},n}(1) \quad \sim \quad \tfrac{1}{2} \frac{\left(\frac{3}{4}\right)^{\frac{n-1}{2}} 2}{\sqrt{\pi \frac{n-1}{2}}} = \frac{\left(\frac{3}{4}\right)^{\frac{n}{2}}}{\sqrt{\frac{3}{4}\pi \frac{n-1}{2}}} \quad \sim \quad p_n \coloneqq \frac{\left(\frac{3}{4}\right)^{\frac{n}{2}}}{\sqrt{\pi n \frac{3}{8}}} \tag{11}$$

5.2 Uniform Ball Model

We derive similarly simple asymptotic expressions in the uniform ball case by approximating $F^{*}_{\texttt{ball},n}(1)$: the CDF expressions at $z = 1$ for each case $* \in$

$\{\texttt{G-}, \texttt{G±}, \texttt{L-}, \texttt{L±}\}$:

$$\begin{aligned}
F^{\texttt{G-}}_{\texttt{ball},n}(1) &= I_{3/4}(\tfrac{n+1}{2}, \tfrac{1}{2}) + I_{1/4}(\tfrac{n+1}{2}, \tfrac{n+1}{2}) &&= \tfrac{3}{2} I_{3/4}(\tfrac{n+1}{2}, \tfrac{1}{2}),\\
F^{\texttt{G±}}_{\texttt{ball},n}(1) &= 2F^{\texttt{G-}}_{\texttt{ball},n}(1) - 2^{-n} &&= 3I_{3/4}(\tfrac{n+1}{2}, \tfrac{1}{2}) - 2^{-n},\\
F^{\texttt{L-}}_{\texttt{ball},n}(1) &= F^{\texttt{G-}}_{\texttt{ball},n}(1) - \tfrac{1}{2} I_{3/4}(\tfrac{n+1}{2}, \tfrac{1}{2}) &&= I_{3/4}(\tfrac{n+1}{2}, \tfrac{1}{2}),\\
F^{\texttt{L±}}_{\texttt{ball},n}(1) &= 2F^{\texttt{L-}}_{\texttt{ball},n}(1) &&= 2I_{3/4}(\tfrac{n+1}{2}, \tfrac{1}{2}).
\end{aligned}$$

Asymptotically the 2^{-n} term is dominated and vanishes by deriving the following asymptotic limit:

$$\lim_{n\to\infty} \frac{2^{-n}}{3I_{3/4}(\frac{n+1}{2}, \frac{1}{2})} = \lim_{n\to\infty} \frac{2^{-n}}{3\frac{2(3/4)^{(n+1)/2}}{\sqrt{\pi(n+1)/2}}} = \lim_{n\to\infty} \sqrt{\pi \tfrac{n+1}{2}} \cdot 3^{-(n+3)/2} = 0.$$

Hence, we can obtain all four asymptotic expressions from their common expression:

$$I_{3/4}(\tfrac{n+1}{2}, \tfrac{1}{2}) \sim \frac{2(\frac{3}{4})^{(n+1)/2}}{\sqrt{\pi(n+1)/2}} = \frac{2(\frac{3}{4})^{n/2}}{\sqrt{2\pi(n+1)/3}} \sim \frac{2(\frac{3}{4})^{n/2}}{\sqrt{2\pi n/3}} = \tfrac{3}{2} p_n$$

Thereby, we prove Lemma 1:

$$\begin{aligned}
F^{\texttt{G-}}_{\texttt{ball},n}(1) &\sim 3 \cdot (\tfrac{3}{4})^{n/2} / \sqrt{2\pi n/3} = \tfrac{9}{4} p_n\\
F^{\texttt{G±}}_{\texttt{ball},n}(1) &\sim 6 \cdot (\tfrac{3}{4})^{n/2} / \sqrt{2\pi n/3} = \tfrac{9}{2} p_n\\
F^{\texttt{L-}}_{\texttt{ball},n}(1) &\sim 2 \cdot (\tfrac{3}{4})^{n/2} / \sqrt{2\pi n/3} = \tfrac{3}{2} p_n\\
F^{\texttt{L±}}_{\texttt{ball},n}(1) &\sim 4 \cdot (\tfrac{3}{4})^{n/2} / \sqrt{2\pi n/3} = 3 p_n
\end{aligned}$$

5.3 Non-Uniform Ball Model

In this section we analyse the asymptotic behaviour in the non-uniform ball model. We first show that we can simplify the four integration regions to (composition of) simple square regions. We then translate the results from our non-uniform ball model in Section 4 from lengths to scaled depths, and derive the asymptotic results proving Lemma 2.

Truncated integration region. We can truncate the integration regions $R_{\texttt{G-}}$ and $R_{\texttt{G±}}$ to a simpler subregion. Namely, for $s \geq \sqrt{1/2}$ and $z \in [s, 1]$, we can show that:

$$[s, 1]^2 \subset R_{\texttt{G±}}(z) \subset R_{\texttt{G-}}(z).$$

Proof. $R_{\texttt{G±}}(z) \subset R_{\texttt{G-}}(z)$ by definition: $g(x, y, z) \in [0, 1] \Rightarrow g(x, y, z) \in [-1, 1]$. Solving $g(x, y, z) \leq 1$ and $g(x, y, z) \geq 0$ we obtain:

$$\frac{x^2 + y^2 - z^2}{2xy} \leq 1 \Leftrightarrow x^2 + y^2 - 2xy \leq z^2 \Leftrightarrow (x - y)^2 \leq z^2 \Leftrightarrow |x - y| \leq |z| = z.$$

Table 3. Log relative error of truncating regions from $[0,1]$ to $[\sqrt{1/2},1]$, i.e. $\log_2(F(\sqrt{1/2})/F(1))$.

n	$F_{\texttt{ball},n}$	$F^{\texttt{G-}}_{\texttt{sphere},n}$	$F^{\texttt{G±}}_{\texttt{ball},n}$	$F^{\texttt{G-}}_{\texttt{ball},n}$	$F^{\texttt{L±}}_{\texttt{ball},n}$	$F^{\texttt{L-}}_{\texttt{ball},n}$
33	−16.500	−12.950	−12.659	−12.659	−12.074	−12.074
65	−32.500	−25.425	−25.073	−25.073	−24.488	−24.488
129	−64.500	−50.329	−49.936	−49.936	−49.351	−49.351
257	−128.50	−100.11	−99.690	−99.690	−99.105	−99.105
513	−256.50	−199.65	−199.22	−199.22	−198.63	−198.63

$$\frac{x^2+y^2-z^2}{2xy} \geq 0 \Leftrightarrow x^2+y^2 \geq z^2.$$

For $\sqrt{1/2} \leq s \leq x,y,z \leq 1$ we see that $x^2+y^2 \geq 2s^2 \geq 1 \geq z \geq z^2$ and thus $g(x,y,z) \geq 0$. Lastly $|x-y| \leq 1-s \leq 1-\sqrt{1/2} < \sqrt{1/2} \leq s \leq z$ and thus $g(x,y,z) \leq 1$. □

Since $R_{\texttt{L±}}(z) = R_{\texttt{L-}}(z) = R_{\texttt{G±}}(z) \cap \{(x,y) : \max(x,y) \geq z\}$, we can easily derive that truncated to $[s,1]^2$, we have for $z \in [s,1]$:

$$\begin{aligned}
&R_{\texttt{L±}}(z) \cap [s,1]^2 = R_{\texttt{L-}}(z) \cap [s,1]^2 \\
=&R_{\texttt{G±}}(z) \cap \{(x,y) : \max(x,y) \geq z\} \cap [s,1]^2 \\
=&[s,1]^2 \cap \{(x,y) : \max(x,y) \geq z\} = [s,1]^2 \setminus [s,z]^2.
\end{aligned}$$

For any input ball distribution $\mathcal{D}$ with length CDF F, for which $F(\sqrt{1/2})/F(1)$ is (asymptotically) negligible, we obtain that truncating the integration regions results in an (asymptotic) approximation for $z \in [\sqrt{1/2},1]$:

$$f^*_{\mathcal{D}}(z) \sim c_* \iint_{T_*} f(x)f(y)E_n(x,y,z)\,\mathrm{d}x\,\mathrm{d}y,$$

where $f = F'$ is the length PDF and c_* is as defined in Lemma 5 ($c_* = 2$ for $\texttt{G±}$ or $\texttt{L±}$ and 1 otherwise) and

$$T_* := \begin{cases} [\sqrt{1/2},1]^2 & * \text{ is } \texttt{G±} \text{ or } \texttt{G-} \\ [\sqrt{1/2},1]^2 \setminus [\sqrt{1/2},z]^2 & * \text{ is } \texttt{L±} \text{ or } \texttt{L-} \end{cases}$$

Note that truncating the integration region is equivalent to truncating the input PDF to the interval $[\sqrt{1/2},1]$, which we rely on below to obtain asymptotic expressions for the output distribution and reduction probability. As numerical evidence, Table 3 shows the relative error when truncating various PDFs from $[0,1]$ to $[\sqrt{1/2},1]$ for growing dimensions, using that $\int_s^1 f(x)\,\mathrm{d}x = F(1)-F(s)$. The relative errors are practically negligible when n corresponds to lattice dimensions typically used in cryptography.

Asymptotic approximations for the global case. Instead of considering the length distribution $\|X\|$, we can also analyse the scaled depth distribution:

$$W \coloneqq -n \ln \|X\|, \quad \|X\| = e^{-W/n}. \tag{12}$$

Recall that for the uniform distribution $X \sim U(\mathcal{B}_n)$, one finds that W has an exponential distribution:

$$\Pr[W > w] = \Pr[\|X\| \leq e^{-w/n}] = (e^{-w/n})^n = e^{-w}.$$

This motivates us to reexamine the truncated double integrals

$$f^*_{\mathcal{D}}(z) = c_* \iint_{T_*} f(x) f(y) \frac{z}{xy} \frac{(1 - g(x,y,z)^2)^{(n-3)/2}}{B(\frac{n-1}{2}, \frac{1}{2})} \,\mathrm{d}x \,\mathrm{d}y, \tag{13}$$

in terms of scaled depths instead of lengths, and translate length PDFs f into scaled depth PDFs $\widehat{f}$ for the asymptotic analysis in this section.

Thus, we analyse the length distribution by a change of variables from length to scaled depth: let $w_x, w_y, w_z \in \mathbb{R}_{\geq 0}$ and define:

$$x \coloneqq e^{-w_x/n}, \quad y \coloneqq e^{-w_y/n}, \quad z \coloneqq e^{-w_z/n},$$

it follows that

$$\mathrm{d}x = (-e^{-w_x/n}/n)\,\mathrm{d}w_x, \quad \mathrm{d}y = (-e^{-w_y/n}/n)\,\mathrm{d}w_y, \quad \mathrm{d}z = (-e^{-w_z/n}/n)\,\mathrm{d}w_z.$$

We define the scaled depth PDFs on $[0, \infty)$ as:

$$\widehat{f}(w_x) \coloneqq f(e^{-w_x/n}) \tfrac{e^{-w_x/n}}{n}, \quad \widehat{f^*_{\mathcal{D}}}(w_z) \coloneqq f^*_{\mathcal{D}}(e^{-w_z/n}) \tfrac{e^{-w_z/n}}{n},$$

so that $f(x)|\,\mathrm{d}x| = \widehat{f}(w_x)|\,\mathrm{d}w_x|$. Note that the interval $(0, 1]$ for f corresponds to $(\infty, 0]$ for $\widehat{f}$, and similarly $[s, 1]$ corresponds to $[-n \ln s, 0]$. Thus for convenience, we have changed the direction and swapped interval endpoints for $\widehat{f}$, causing a negation that cancels with the negation in the Jacobian $\mathrm{d}x = (-e^{-w_x/n}/n)\,\mathrm{d}w_x$. This implies that each $\widehat{f}$ is a probability density in its own right, so that the reduction probability can be read off directly from the scaled depth density:

$$\int_0^\infty \widehat{f}(w_x)\,\mathrm{d}w_x = \int_0^1 f(x)\,\mathrm{d}x, \qquad \int_0^\infty \widehat{f^*_{\mathcal{D}}}(w_z)\,\mathrm{d}w_z = \int_0^1 f^*_{\mathcal{D}}(z)\,\mathrm{d}z = F^*_{\mathcal{D}}(1).$$

E.g, for the uniform ball distribution $f_{\mathtt{ball},n}(x) = nx^{n-1}$ we obtain $\widehat{f}_{\mathtt{ball},n}(w) = e^{-w}$, i.e., exactly Exp(1) (cf. Eq. (2)). When f is truncated to $[s, 1]$, then by convention we also truncate $\widehat{f}$ to $[0, -n \ln s]$ (and is thus zero on $(-n \ln s, \infty)$).

We use this to transform Eq. (13) for the global cases $G\pm, G-$ by a change of variables into:

$$\widehat{f^*_{\mathcal{D}}}(w_z) = \frac{c_*}{n} \iint_{[0,\infty)^2} \widehat{f}(w_x)\widehat{f}(w_y)\widehat{h}(w_x, w_y, w_z) \frac{(1 - \widehat{g}(w_x, w_y, w_z)^2)^{(n-3)/2}}{B(\frac{n-1}{2}, \frac{1}{2})} \,\mathrm{d}w_x \,\mathrm{d}w_y,$$

$$\text{where } \widehat{g}(w_x, w_y, w_z) \coloneqq g(e^{-w_x/n}, e^{-w_y/n}, e^{-w_z/n}),$$

$$\widehat{h}(w_x, w_y, w_z) \coloneqq \frac{z}{xy} e^{-w_z/n} = e^{(w_x + w_y - 2w_z)/n}. \tag{14}$$

Note that $\widehat{h}$ is a single exponential and can asymptotically be ignored by an invocation of the dominated convergence theorem: for any w_x, w_y, w_z, $\lim_{n\to\infty} \widehat{h}(w_x, w_y, w_z) = 1$. We therefore shift our focus to the factor

$$(1 - \widehat{g}(w_x, w_y, w_z)^2)^{(n-3)/2}.$$

The function $\widehat{g}$ likewise has a closed form expression in the scaled depths, writing $\delta \coloneqq w_x - w_y$ and $\sigma \coloneqq w_x + w_y - 2w_z$:

$$\begin{aligned}\widehat{g}(w_x, w_y, w_z) &= \frac{e^{-2w_x/n} + e^{-2w_y/n} - e^{-2w_z/n}}{2e^{-(w_x+w_y)/n}} \\ &= \tfrac{1}{2}e^{(-w_x+w_y)/n} + \tfrac{1}{2}e^{(-w_y+w_x)/n} - \tfrac{1}{2}e^{(w_x+w_y-2w_z)/n} \\ &= \cosh\left(\tfrac{\delta}{n}\right) - \tfrac{1}{2}e^{\sigma/n} = \cosh\left(\tfrac{\delta}{n}\right) - \tfrac{1}{2}\widehat{h}(w_x, w_y, w_z).\end{aligned} \tag{15}$$

Expanding the above closed form shows that $1 - \widehat{g}^2 = \frac{3}{4}(1 + \frac{2\sigma}{3n} + O(n^{-2}))$, after which the limit $\lim_{n\to\infty}(1 + t/n)^n = e^t$ applies and we obtain Lemma 6:

Lemma 6. *Let $w_x, w_y, w_z \in \mathbb{R}_{\geq 0}$ then asymptotically as $n \to \infty$:*

$$\left(1 - \widehat{g}(w_x, w_y, w_z)^2\right)^{(n-3)/2} \quad \sim \quad \left(\tfrac{3}{4}\right)^{(n-3)/2} \cdot e^{w_x/3} \cdot e^{w_y/3} \cdot e^{-2w_z/3}.$$

Remark 1. This asymptotic equivalence in Lemma 6 holds pointwise for any $w_x, w_y, w_z \in \mathbb{R}_{\geq 0}$, in which case $x, y, z \to 1$ as $n \to \infty$. However, the equivalence fails when evaluating pointwise for any fixed $x, y, z \in [0, 1)$ (and defining $w_x = -n \ln x$, etc.) as then $w_x, w_y, w_z \to \infty$ as $n \to \infty$.

Proof. We expand $\widehat{g}(w_x, w_y, w_z)$ up to $O(n^{-2})$, starting from its closed form expression and using $\cosh(\delta/n) = 1 + O(n^{-2})$ and $e^{\sigma/n} = 1 + \frac{\sigma}{n} + O(n^{-2})$. Note that the cosh term contributes a constant 1, and δ only at order n^{-2}, thus the leading behaviour at order n^{-1} is by σ alone:

$$\begin{aligned}\widehat{g}(w_x, w_y, w_z) &= \cosh\left(\tfrac{\delta}{n}\right) - \tfrac{1}{2}e^{\sigma/n} = \left(1 + O(n^{-2})\right) - \tfrac{1}{2}\left(1 + \tfrac{\sigma}{n} + O(n^{-2})\right) \\ &= \tfrac{1}{2}\left(1 - \tfrac{\sigma}{n} + O(n^{-2})\right)\end{aligned}$$

We then square it using $(1 + x + O(x^2))^2 = 1 + 2x + O(x^2)$:

$$\widehat{g}(w_x, w_y, w_z)^2 = \tfrac{1}{4} - \tfrac{\sigma}{2n} + O(n^{-2}).$$

Hence, $(1 - \widehat{g}(w_x, w_y, w_z)^2)^{(n-3)/2}$ can be expanded up to $O(n^{-2})$ as:

$$\begin{aligned}\left(1 - \widehat{g}(w_x, w_y, w_z)^2\right)^{(n-3)/2} &= \left(\tfrac{3}{4} + \tfrac{\sigma}{2n} + O(n^{-2})\right)^{(n-3)/2} \\ &= (\tfrac{3}{4})^{(n-3)/2} \cdot \left(1 + \tfrac{4}{3}\tfrac{\sigma}{2n}\tfrac{n-3}{n-3} + O(n^{-2})\right)^{(n-3)/2} \\ &= (\tfrac{3}{4})^{(n-3)/2} \cdot \left(1 + \tfrac{1}{3}\tfrac{\sigma}{(n-3)/2} + O(n^{-2})\right)^{(n-3)/2}\end{aligned}$$

Now the desired result follows from observing the limit of the last factor:

$$\lim_{n\to\infty}\left(1 + \frac{\sigma/3}{(n-3)/2} + O(n^{-2})\right)^{(n-3)/2} = e^{\sigma/3} = e^{(w_x+w_y-2w_z)/3}.$$

□

The restrictions on the family of scaled depth PDFs stated in Lemma 2 is captured by the following definition:

Definition 1 (Admissible family). *A family of scaled depth PDFs* $\{\widehat{f}_n\}_{n\geq 3}$ *is called admissible if it satisfies the following requirements:*

- *the limit* $\widehat{f}$ *exists pointwise for almost every* w *and is a scaled depth PDF*
- *there exists an integrable* v *such that* $\widehat{f}_n(w) \leq v(w)$ *for all* n *and almost all* w
- *for this* v *the integral* $\int_0^\infty v(w)e^{w/3}\,\mathrm{d}w$ *exists and is finite*

Remark 2. The family of non-truncated scaled depth PDFs obtained by transforming the uniform length PDFs $f_n(x) = nx^{n-1} \to \widehat{f}_n(w) = e^{-w}$ is constant and admissible.

Now we have pointwise asymptotic limits for $\widehat{g}$ and $\widehat{h}$ that can be substituted into Eq. (14):

Lemma 7. *Given an admissible family* $\{\widehat{f}_n\}_{n\geq 3}$ *with the limit* $\widehat{f}$*; let* $\mathcal{D}_n$ *be the distribution in* $\mathcal{B}_n$ *corresponding to* $\widehat{f}_n$*, then as* $n \to \infty$*:*

$$\begin{aligned}\widehat{f}^*_{\mathcal{D}_n}(w_z) &\sim \frac{c_*}{n}\iint\limits_{[0,\infty)^2} \widehat{f}(w_x)\widehat{f}(w_y)\frac{\left(\frac{3}{4}\right)^{(n-3)/2} e^{(w_x+w_y-2w_z)/3}}{B(\frac{n-1}{2},\frac{1}{2})}\,\mathrm{d}w_x\,\mathrm{d}w_y \\ &= e^{-2w_z/3}\frac{c_*\left(\frac{3}{4}\right)^{(n-3)/2}}{nB(\frac{n-1}{2},\frac{1}{2})}\left(\int_0^\infty \widehat{f}(w_x)e^{w_x/3}\,\mathrm{d}w_x\right)^2. \qquad (16)\end{aligned}$$

Proof. Equation (14) can be represented as the product of a term only depending on n

$$\frac{c_*\left(\frac{3}{4}\right)^{(n-3)/2}}{nB(\frac{n-1}{2},\frac{1}{2})} \qquad (17)$$

and a term depending on n, w_x, w_y, w_z

$$\iint\limits_{[0,\infty)^2} \widehat{f}_n(w_x)\widehat{f}_n(w_y)\widehat{h}\left(\tfrac{4}{3}(1-\widehat{g}^2)\right)^{(n-3)/2}\,\mathrm{d}w_x\,\mathrm{d}w_y, \qquad (18)$$

where we write $\widehat{h}$ for $\widehat{h}(w_x, w_y, w_z)$ and $\widehat{g}$ for $\widehat{g}(w_x, w_y, w_z)$.

Equation (17) converges to 0 as $n \to \infty$ since the numerator decays exponentially while the decay of denominator is polynomially bounded. For now, we merely assume that Eq. (18) also converges to a limit. It follows that we can ignore Eq. (17) and focus on Eq. (18) to prove an asymptotic equivalence.

The dominated convergence theorem allows us to apply the pointwise limits of $\widehat{h}$, and $(1-\widehat{g}(w_x, w_y, w_z)^2)^{(n-3)/2}$ from Lemma 6, and thus obtain the desired equivalence. However, the theorem requires that there exists an integrable

function $u(w_x, w_y, w_z)$ that dominates the integrand of Eq. (18) for every $n \geq 3$. First, we claim

$$0 \leq \widehat{h}(\tfrac{4}{3}(1-\widehat{g}^2))^{(n-3)/2} \leq e^{(w_x+w_y-2w_z)/3} \quad \text{for } n \geq 3,$$

this follows from $\widehat{g} = \cosh\left(\frac{\delta}{n}\right) - \frac{1}{2}\widehat{h}(w_x, w_y, w_z)$, which implies $\widehat{g} \geq 1 - \frac{\widehat{h}}{2}$ as $\cosh \geq 1$. Substituting $\widehat{g}$ in $1 - \widehat{g}^2$ gives:

$$1 - \widehat{g}^2 \leq 1 - (1 - \tfrac{\widehat{h}}{2})^2 = \widehat{h} - \tfrac{\widehat{h}^2}{4}.$$

Using Bernoulli's inequality $1 + ax \leq (1+x)^a$ for $a = -1/3$ and $x = \widehat{h} - 1$, we can obtain $\frac{4}{3} - \frac{1}{3}\widehat{h} \leq \widehat{h}^{-1/3}$ and multiplying by $\widehat{h}$ gives:

$$\tfrac{4}{3}(1-\widehat{g}^2) \leq \tfrac{4}{3}(\widehat{h} - \widehat{h}^2/4) \leq \widehat{h}^{2/3}.$$

Now it follows for $n \geq 3$ that:

$$\widehat{h}(\tfrac{4}{3}(1-\widehat{g}^2))^{(n-3)/2} \leq \widehat{h}^{\left(1+\frac{2}{3}\frac{n-3}{2}\right)} = \widehat{h}^{n/3} = e^{(w_x+w_y-2w_z)/3},$$

which turns our earlier assumption about Eq. (18) having a limit into the condition that

$$\int_0^\infty \widehat{f}_n(w_x) e^{w_x/3}\, \mathrm{d}w_x < \infty, \tag{19}$$

which is true due to $\widehat{f}_n$ being an element of an admissible family.

We define

$$u(w_x, w_y, w_z) \coloneqq v(w_x)v(w_y)e^{(w_x+w_y-2w_z)/3},$$

where v is the integrable upper bound of the family. Then u dominates the integrand of Eq. (18) for every such n

$$u(w_x, w_y, w_z) = v(w_x)v(w_y)e^{(w_x+w_y-2w_z)/3} \tag{20}$$

$$\geq \widehat{f}_n(w_x)\widehat{f}_n(w_y)\widehat{h}\left(\tfrac{4}{3}(1-\widehat{g}^2)\right)^{(n-3)/2} \tag{21}$$

and is integrable. □

Proposition 1. *The shape of the output distribution for any admissible family converges to the unique limit* Exp(2/3)*, an exponential distribution with parameter* 2/3.

This proves the first part of Lemma 2.

We now analyse the asymptotic behaviour of the reduction probability for two input distributions of w_x, w_y:

- Exp(1) - the uniform ball distribution (exactly, at every n)
- Exp(2/3) - the stable output distribution (asymptotically)

Note that $-n \ln s \to \infty$ as $n \to \infty$, so asymptotically we integrate over the full interval $[0, \infty)$ and ignore zero-extension. The PDF $\widehat{f}_a$ for $\mathrm{Exp}(a)$, the exponential distribution with parameter a is:

$$\widehat{f}_a(w_x) = ae^{-aw_x}, \quad \int_0^\infty ae^{-aw_x}\,\mathrm{d}w_x = \left[-e^{-aw_x}\right]_0^\infty = 1.$$

It corresponds to the length PDF $f_a(x) = anx^{an-1}$ with CDF x^{an} (of which the uniform ball is the case $a = 1$). The only term in Eq. (16) that depends on $\widehat{f}_a$ is the square of

$$\int_0^\infty \widehat{f}_a(w_x)e^{w_x/3}\,\mathrm{d}w_x,$$

which converges if $a > 1/3$:

$$\int_0^\infty \widehat{f}_a(w_x)e^{w_x/3}\,\mathrm{d}w_x = \int_0^\infty ae^{-aw_x}e^{w_x/3}\,\mathrm{d}w_x = \frac{3a}{3a-1}\left[-e^{-aw_x+w_x/3}\right]_0^\infty = \frac{3a}{3a-1}.$$

Then, for the input scaled depth distribution $\widehat{f}_a$ with $a > \frac{1}{3}$, the overall reduction probability can be found as:

$$\begin{aligned}
\int_0^\infty \widehat{f}^*(w_z)\,\mathrm{d}w_z \sim& \int_0^\infty e^{-2w_z/3}\,\mathrm{d}w_z \cdot \frac{c_*\left(\frac{3}{4}\right)^{(n-3)/2}}{nB(\frac{n-1}{2},\frac{1}{2})} \cdot \left(\frac{3a}{3a-1}\right)^2 \\
=& \frac{3}{2} \cdot \frac{c_*\left(\frac{3}{4}\right)^{(n-3)/2}}{nB(\frac{n-1}{2},\frac{1}{2})} \cdot \left(\frac{3a}{3a-1}\right)^2 = \frac{2c_*\left(\frac{3}{4}\right)^{(n-1)/2}}{nB(\frac{n-1}{2},\frac{1}{2})}\left(\frac{3a}{3a-1}\right)^2 \\
\sim& \frac{2c_*\left(\frac{3}{4}\right)^{(n-1)/2}}{n\sqrt{2\pi/n}}\left(\frac{3a}{3a-1}\right)^2 = \frac{c_*\left(\frac{3}{4}\right)^{n/2}}{\sqrt{\pi n 3/8}}\left(\frac{3a}{3a-1}\right)^2 \\
=& p_n c_* \left(\frac{3a}{3a-1}\right)^2
\end{aligned}$$

This proves the second part of Lemma 2.

We define the asymptotic advantage of a case $*$ with input distribution $\mathrm{Exp}(a)$, over the sphere model:

$$\alpha_a(*) \coloneqq \lim_{n\to\infty} \frac{\int_0^\infty \widehat{f}^*(w_z)\,\mathrm{d}w_z}{F^{\texttt{G-}}_{\texttt{sphere},n}(1)} = \lim_{n\to\infty} \frac{\int_0^\infty \widehat{f}^*(w_z)\,\mathrm{d}w_z}{p_n}, \tag{22}$$

For $a = 1$ (the uniform distribution) we obtain $2(\frac{3}{3-1})^2 p_n = \frac{9}{2}p_n$ for `G±`, and $\frac{9}{4}p_n$ for `G-`, which corresponds to the asymptotic advantages we found using the explicit formulae for $F^{\texttt{G±}}_{\texttt{ball},n}$ and $F^{\texttt{G-}}_{\texttt{ball},n}$ in Section 3. For $a = 2/3$ (the stable distribution) we obtain $2(\frac{2}{2-1})^2 = 8p_n$ for `G±`, and $4p_n$ for `G-`.

Asymptotic approximations for the local case. Translating Eq. (16) to `L-` or `L±` merely requires accounting for the smaller integration region for w_x, w_y,

Table 4. Global Advantages. The asymptotic advantage of global cases over the sphere model α_a (cf. Eq. (22)). For the input distributions, 'Uniform' refers to $\widehat{f}_1$ ($a = 1$) and 'Stable' to $\widehat{f}_{2/3}$ ($a = 2/3$).

Case (*)	Input Distribution (a)	$\alpha_a(*)$
G±	Uniform	$\frac{9}{2}$
	Stable	8
G-	Uniform	$\frac{9}{4}$
	Stable	4

$[0,\infty)^2 \setminus [w_z,\infty)^2$ for $w_z \in [0,\infty)$. We achieve this by subtracting the density of the event that a global reduction occurs, which is not a local reduction from *Eq.* (16), i.e., the case that a reduction occurs when $w_x > w_z \wedge w_y > w_z$.

This density is captured by the term

$$e^{-w_z \frac{2}{3}} \frac{c_*\left(\frac{3}{4}\right)^{\frac{n-3}{2}}}{nB(\frac{n-1}{2},\frac{1}{2})} \left(\int_{w_z}^{\infty} \widehat{f}(w_x) e^{\frac{w_x}{3}} \,\mathrm{d}w_x\right)^2. \tag{23}$$

For the squared term (which is no longer independent of w_z), we apply similar reasoning as before

$$\begin{aligned}\left(\int_{w_z}^{\infty} \widehat{f}_a(w_x) e^{w_x/3} \,\mathrm{d}w_x\right)^2 &= \left(\int_{w_z}^{\infty} a e^{-aw_x} e^{w_x/3} \,\mathrm{d}w_x\right)^2 \\ &= \left(\frac{3a}{3a-1}\left[-e^{-aw_x+w_x/3}\right]_{w_z}^{\infty}\right)^2 \\ &= \left(\frac{3a}{3a-1}\right)^2 e^{2w_z(\frac{1}{3}-a)},\end{aligned}$$

which, combined with Eq. (23), gives us the integrand for calculating the reduction probability

$$e^{-2aw_z}\left(\frac{3a}{3a-1}\right)^2 \frac{c_*\left(\frac{3}{4}\right)^{\frac{n-3}{2}}}{nB(\frac{n-1}{2},\frac{1}{2})}.$$

Finally, we integrate over w_z to obtain the probability of a global reduction that is not local and express it as a multiple of p_n

$$\begin{aligned}\int_0^{\infty} e^{-2aw_z} \,\mathrm{d}w_z \left(\frac{3a}{3a-1}\right)^2 \frac{c_*\left(\frac{3}{4}\right)^{\frac{n-3}{2}}}{nB(\frac{n-1}{2},\frac{1}{2})} &= \frac{1}{2a}\left(\frac{3a}{3a-1}\right)^2 \frac{c_*\left(\frac{3}{4}\right)^{\frac{n-3}{2}}}{nB(\frac{n-1}{2},\frac{1}{2})} \\ &\sim \frac{1}{3a} p_n c_* \left(\frac{3a}{3a-1}\right)^2,\end{aligned}$$

which only differs from the probability of a global reduction by the factor $\frac{1}{3a}$. Consequently, the advantage $\alpha_a(*)$ for (L±, L-) with input distribution $\mathrm{Exp}(a)$,

over the sphere model is obtained by multiplying the advantage of the corresponding global case $(\alpha_a(\texttt{G±}), \alpha_a(\texttt{G-}))$ with

$$1 - \frac{1}{3a} = \frac{3a-1}{3a}.$$

For the uniform distribution, this factor is $\frac{2}{3}$ and for the stable distribution $\frac{1}{2}$. We combine these factors with the global advantages from Table 4 and display the results in Table 5. Note that stable refers to the global stable distribution, since following our approach does not result in a stable distribution for the local case.

Table 5. Local Advantages. The asymptotic advantage of local cases over the sphere model α_a (cf. Eq. (22)). For the input distributions, 'Uniform' refers to $\widehat{f}_1$ ($a = 1$) and 'Stable' to $\widehat{f}_{2/3}$ ($a = 2/3$). Note that stable refers to the global stable distribution. We do not present a local stable distribution.

Case (*)	**Input Distribution (a)**	$\alpha_a(*)$
L±	Uniform	3
	Stable	4
L-	Uniform	$\frac{3}{2}$
	Stable	2

References

[ABD+21] Roberto Avanzi, Joppe Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, Gregor Seiler, and Damien Stehlé. Crystals-kyber (version 3.01) – submission to round 3 of the nist post-quantum project. Submission to the NIST PQC project, January 2021. URL: https://pq-crystals.org/kyber/data/kyber-specification-round3-20210131.pdf.

[AGPS20] Martin R. Albrecht, Vlad Gheorghiu, Eamonn W. Postlethwaite, and John M. Schanck. Estimating quantum speedups for lattice sieves. In Shiho Moriai and Huaxiong Wang, editors, *Advances in Cryptology – ASIACRYPT 2020, Part II*, volume 12492 of *Lecture Notes in Computer Science*, pages 583–613, Daejeon, South Korea, December 7–11, 2020. Springer, Cham, Switzerland. doi:10.1007/978-3-030-64834-3_20.

[DLMF] *NIST Digital Library of Mathematical Functions*. https://dlmf.nist.gov/, Release 1.2.6 of 2026-03-15. F. W. J. Olver, A. B. Olde Daalhuis, D. W. Lozier, B. I. Schneider, R. F. Boisvert, C. W. Clark, B. R. Miller, B. V. Saunders, H. S. Cohl, and M. A. McClain, eds. URL: https://dlmf.nist.gov/.

[dv25] Koen de Boer and Wessel P. J. van Woerden. Lattice-based cryptography: A survey on the security of the lattice-based NIST finalists. Cryptology ePrint Archive, Report 2025/304, 2025. URL: https://eprint.iacr.org/2025/304.

[FBB+15] Robert Fitzpatrick, Christian H. Bischof, Johannes Buchmann, Özgür Dagdelen, Florian Göpfert, Artur Mariano, and Bo-Yin Yang. Tuning GaussSieve for speed. In Diego F. Aranha and Alfred Menezes, editors, *Progress in Cryptology - LATINCRYPT 2014: 3rd International Conference on Cryptology and Information Security in Latin America*, volume 8895 of *Lecture Notes in Computer Science*, pages 288–305, Florianópolis, Brazil, September 17–19, 2015. Springer, Cham, Switzerland. doi:10.1007/978-3-319-16295-9_16.

[KM63] Maurice George Kendall and Patrick Alfred Pierce Moran. *Geometrical Probability*. Griffin's Statistical Monographs & Courses. Griffin, London, 1963. https://archive.org/details/geometricalproba033077mbp.

[Li10] S. Li. Concise formulas for the area and volume of a hyperspherical cap. *Asian Journal of Mathematics & Statistics*, 4(2):66–70, 2010. doi:10.3923/ajms.2011.66.70.

[NV08] Phong Q. Nguyen and Thomas Vidick. Sieve algorithms for the shortest vector problem are practical. *J. Math. Cryptol.*, 2(2):181–207, 2008. doi:10.1515/JMC.2008.009.