New Practical Algorithms for the Approximate Shortest Lattice Vector

Claus Peter Schnorr

Fachbereiche Mathematik/Informatik,
Universität Frankfurt, PSF 41932,
D-60054 Frankfurt am Main, Germany.
schnorr@cs.uni-frankfurt.de
http://www.mi.informatik.uni-frankfurt.de/

Preliminary Report

Abstract. We present a practical algorithm that given an LLL-reduced lattice basis of dimension n, runs in time $O(n^3(k/6)^{k/4}+n^4)$ and approximates the length of the shortest, non-zero lattice vector to within a factor $(k/6)^{n/(2k)}$. This result is based on reasonable heuristics. Compared to previous practical algorithms the new method reduces the proven approximation factor achievable in a given time to less than its fourth-th root. We also present a sieve algorithm inspired by Ajtai, Kumar, Sivakumar [AKS01].

1 Introduction and Summary

History. The problem of finding a shortest, non-zero lattice vector in a lattice of dimension n is a landmark problem in complexity theory. This problem is polynomial time for fixed dimension n, it is NP-complete for varying n. For simplicity, we consider integer lattices of dimension n in $\mathbf{Z}^n$, given by a lattice basis consisting of vectors of Euclidean length $2^{O(n)}$. Using the famous LLL-algorithm of Lenstra, Lenstra, Lovász (1982), Kannan (1983) proposed an algorithm that finds the shortest lattice vector in time $n^{O(n)}$, Helfrich (1985) improved the time bound to $n^{n/2+o(n)}$. Recently [AKS01] present a probabilistic algorithm with time and space bound $2^{O(n)}$, at present that method is still impractical.

We present a novel algorithm that produces an approximate shortest lattice vector by iterating random sampling of short lattice vectors. It finds a shortest lattice vector to within the factor $(k/6)^{n/(2k)}$ and runs in time $O(n^3(k/6)^{k/4}+n^4)$. This algorithm is practical and space efficient, theoretically it outperforms all other known algorithms. We show how to speed up random sampling via the birthday paradox. This reduces the time to $O(n^3(k/3)^{k/8}+n^4)$ at the expense of storing $n(k/3)^{k/8}$ lattice vectors. We also present, a nearly practical sieve algorithm, inspired by [AKS01] and adapted to the problem of *approximating* the shortest lattice vector. Our analysis uses reasonable heuristic assumptions.

Summary and Comparison of the New Algorithms. The next table shows and compares the performance of the new algorithms for approximating the shortest lattice vector. Approximating the shortest lattice vector to within an *approximation factor* c means to find a non-zero lattice vector with at most c-times the minimal possible length.

	time	space/n^2	approx. factor
1. random sampling	$n^3(k/6)^{k/4}$	1	$(k/6)^{n/2k}$
for $n \geq 160$	$n^3 2^{13}$	1	1.026^n
2. birthday sampl.	$n^3(k/3)^{k/8}$	$(k/3)^{k/8}$	$(k/3)^{n/2k}$
3. our sieve	$n^3\, 2^{0.835\,k}$	$2^{0.835\,k}$	$k^{3n/4k}$
for $k = 60$	$n^3 2^{50}$	2^{50}	1.053^n
4. primal/dual (Koy)	$n^2 k^{k/2+o(k)}$	n^2	$(k/6)^{n/k}$
for $k = 22$	$n^2 2^{49}$	1	1.06^n
5. Schnorr 1987	$n^2 k^{k+o(k)}$	1	$(k/3)^{n/k}$
for $k = 14$	$n^2 2^{53}$	1	1.12^n
6. AKS 2001	$n^2 2^{O(k)}$	$2^{O(k)}$	$(k/6)^{n/k}$

The time bounds count arithmetic steps using integers of bit length $O(n)$, assuming a given basis consisting of integer vectors of length $2^{O(n)}$. More precisely, all time bounds are of the form $O(\ *\ + n^4)$ with a constant factor and an additive term n^4 related to LLL-type reduction. The constants $2^{13}, 2^{50}, 2^{49}, 2^{53}$ are method specific. The parameter $k,\ 1 < k \leq n$ can be freely chosen. The entry c under space/n^2 means that $c + O(n)$ lattice vectors, consisting of $c \cdot n + O(n^2)$ integers, need to be stored. This requires to store $O(c \cdot n^2 + n^3)$ bits.

The proven approximation factor $(k/6)^{n/2k}$ of random sampling is about the fourth-th root of the proven factor achievable in the same time by Koy's primal-dual method, the best practical, previous algorithm. Algorithms 4. and 5. yield in practice smaller approximation factors than the proven ones. The approximation factors of methods 4, 5. 6. assume the unproven bound $\gamma_k \leq k/6$ for $k \geq 24$ for the HERMITE constant γ_k of dimension k. [1] Random sampling is still to be implemented. Its theoretical performance beats by far all other known practical methods. Surprisingly, the proven approximation factor 1.026^n of $n^3 2^{13}$-time random sampling is pretty near to the ones observed in practice by the algorithms 4. and 5. Possibly, this explains why methods 4. and 5. perform better in practice than expected from the theoretic analysis.

Our sieve yields for $k = n - 1$ the approximation factor n within average time $2^{0.835\,n+o(n)}$ under the assumption that there are many short

[1] The Hermite constant γ_k is the maximum value $\lambda_1(L)^2(\det(L)^{-2/k}$, where L ranges over all lattices of dimension k and $\lambda_1(L)$ denotes the length of the shortest, non-zero vector in L.

lattice vectors. A drawback is the space requirement, $2^{0.835\,n+o(n)}$ lattice vectors must be stored. Asymptotically the new sieve performs for $k = \frac{n}{3}$ on average $O(n^3 2^{0.278n+o(n)})$ steps and approximates the shortest lattice vector to within a factor $n^{9/4}$. This indicates that approximating the shortest lattice vector to within a factor $n^{9/4}$ is easier than computing the shortest lattice vector exactly.

Our sieve finds a basis with the remarkable property that $\|b_1\|/\|\widehat{b}_n\| \leq n$. That property seems not even to hold for lattice bases that are reduced in the very strong sense of HERMITE AND KORKIN-ZOLOTAREV. The latter bases merely satisfy that $\|b_1\|/\|\widehat{b}_n\| \leq n^{(1+\ln 2)/2}$, see [S87],[LLS 90].

The [AKS01] algorithm has the best assymptotic time bound $2^{O(n)}$ for a probabilistic algorithm that finds the shortest lattice vector. At present this method is impractical as the exponent $O(n)$ is about $30\,n$. Method 4. is impractical for $k \geq 32$ as it requires to find shortest lattice vectors for lattices of dimension $2k$ while KOY's primal/dual method (unpublished) uses shortest lattice vectors in dimension k. The approximation factor $(k/6)^{n/k}$ of 6. comes from combining the AKS-sieve with 4.

The following cryptosystems may be affected by current and further progress in lattice basis reduction: NTRU, RSA, Factoring based cryptosystems, DL-cryptosystems with groups of unity. These cryptosystems can be broken by very short lattice vectors in high dimensional lattices, see [HPS98] for NTRU and [S91] for factoring and the DL. LLL-type reduction is now feasible in these dimensions due to Koy, Schnorr [KS01a,KS01b]. The random sampling method marks an important progress towards our goal of finding very short lattice vectors efficiently.

Notation. An ordered set of linearly independent vectors $b_1, ..., b_n \in \mathbf{Z}^m$ is a *basis* of the *lattice* $\sum_{i=1}^n b_i \mathbf{Z} \subset \mathbf{Z}^m$, consisting of all linear integer combinations of $b_1, ..., b_n$. For simplicity we will focus on the case $n = m$. The *orthogonalization vectors* $\widehat{b}_1, ..., \widehat{b}_n$ and the *Gram-Schmidt coefficients* $\mu_{i,j}$, $1 \leq i, j \leq n$, associated with the basis $b_1, ..., b_n$ satisfy for $i = 1, ..., n$:

$$b_i = \sum_{j=1}^i \mu_{i,j} \widehat{b}_j, \qquad \mu_{i,i} = 1, \qquad \mu_{i,j} = 0 \ \text{ for } \ j > i.$$

For the Euclidean inner product $\langle\ ,\ \rangle$ we have that

$$\mu_{i,j} = \langle b_i, \widehat{b}_j \rangle / \langle \widehat{b}_j, \widehat{b}_j \rangle, \qquad \langle \widehat{b}_i, \widehat{b}_j \rangle = 0 \text{ for } i \neq j.$$

Let $\|b\| = \langle b, b \rangle^{\frac{1}{2}}$ denote the Euclidean length of a vector $b \in \mathbf{R}^n$. A vector $b = \sum_{i=1}^n \mu_i \widehat{b}_i$ satifies $\|b\|^2 = \sum_{i=1}^n |\mu_i|^2 \|\widehat{b}_i\|^2$. Let λ_1 denote the length of the shortest non-zero lattice vector of a given lattice. For simplicity, let the given lattice basis be nicely bounded so that $\max_i \|b_i\| = 2^{O(n)}$.

It is known from [LLL82] that a given lattice basis can be transformed into an LLL-reduced lattice basis $b_1, ..., b_n$ satisfying $\|b_1\|^2 \leq 2^n \lambda_1^2$ in

polynomial time $n^{O(1)}$. Actually, an approximation factor $(\frac{4}{3}+\varepsilon)^{\frac{n}{2}}$ can be achieved in polynomial time for arbitrary small $\varepsilon > 0$. Recently [KS01a] proposes an LLL-type reduction in time $O(n^3 \log n)$ realizing the approximation factor $(\frac{4}{3}+\varepsilon)^{\frac{n}{2}}$.

2 Random Sampling of Short Vectors

Previous algorithms for the approximate shortest lattice vector generate lattice vectors $b = \sum_{i=1}^{j} \mu_i \widehat{b}_i$ for some $1 < j < n$ such that $|\mu_{j-1}|, ..., |\mu_{j-k}|$ are particularly small, and $|\mu_j| \neq 0$. The goal is to find some $b \in L$ so that $\sum_{i=j-k}^{j} |\mu_i|^2 \|\widehat{b}_i\|^2 < \|\widehat{b}_{j-k}\|^2$. In that case replacing b_{j-k} by b yields a shorter vector $\widehat{b}_{j-k}$.

The new method generates lattice vectors $b = \sum_{i=1}^{n} \mu_i \widehat{b}_i$ such that $|\mu_1|, |\mu_2|, ..., |\mu_k|$ are particularly small. The goal is to find some $b \in L$ so that $\|b\|^2 = \sum_{i=1}^{n} |\mu_i|^2 \|\widehat{b}_i\|^2 < \|b_1\|^2$. In that case the basis vector b_1 is replaced by the shorter vector b. Importantly, the initial vectors $\widehat{b}_1, ..., \widehat{b}_k$ are longer than vectors $\widehat{b}_i$ for large i, so small coefficients $|\mu_i|$ for small i have a bigger impact than those for large i.

The Sampling Method. Let $1 \leq k' < n$ be constant. Suppose we are given an LLL–reduced lattice basis of dimension n. We sample lattice vectors $b = \sum_{i=1}^{n} t_i b_i = \sum_{i=1}^{n} \mu_i \widehat{b}_i$ satisfying

$$|\mu_i| \leq \begin{cases} \frac{1}{2} \text{ for } i \leq n - k' \\ 1 \text{ for } n - k' < i < n \end{cases}, \qquad \mu_n \in \{1, 2\}. \tag{1}$$

There are at least $2^{k'}$ distinct lattice vectors b of this form. The sampling algorithm (SAL) below generates a vector b in time $O(n^2)$. If the sampled vector satisfies $\|b\|^2 \leq \delta \|b_1\|^2$ for some constant $\delta < 1$ we extend b to an LLL-reduced basis with $b_1 = b$ and we iterate the sampling. As an LLL-reduced basis satisfies $\|b_1\|^2 \leq 2^{n-1} \lambda_1^2$ there are at most $\frac{n-1}{2} \log_{(1/\delta)}(2)$ iterations.

Sampling Algorithm (SAL).

Given a lattice basis $b_1, ..., b_n$ with coefficients $\mu_{i,j}$ the algorithm generates a lattice vector $b = \sum_{i=1}^{n} \mu_i \widehat{b}_i$ satisfying (1).

1. Select $\mu_n \in \{1, 2\}$, $b := \mu_n b_n$
   $\mu_j := \mu_n \mu_{n,j}$ for $j = 1, ..., n-1$.
2. FOR $i = n-1, ..., 1$ DO
   Select $\mu \in \mathbf{Z}$ such that
   $$|\mu_i - \mu| \leq \begin{cases} \frac{1}{2} \text{ for } i \leq n - k' \\ 1 \text{ for } i > n - k' \end{cases}, \tag{2}$$
   $b := b - \mu b_i$,
   $\mu_j := \mu_j - \mu \mu_{i,j}$ for $j = 1, ..., i$.

OUTPUT b, $\mu_1, ..., \mu_n$ satisfying $b = \sum_{i=1}^{n} \mu_i \widehat{b}_i$.

The coefficient μ_i is updated $n-i$ times. We assume that this leads to a nearly uniform distribution of the μ_i, at least for small i. That near uniformity is crucial for our method. The random behaviour for large i is less important as the contribution $|\mu_i|^2\|\widehat{b}_i\|^2$ to the length square of b is minor. We make the heuristic

Randomness Assumption (RA). Let the μ_i of the sampled vectors $b = \sum_{i=1}^{n} \mu_i \widehat{b}_i$ be uniformly distributed over the interval $[-\frac{1}{2}, \frac{1}{2}]$ for $i \le n-k'$ resp. the interval $[-1, 1]$ for $i > n-k'$, and let the μ_i be mutually statistically independent for distinct i.

Lemma 1. *For uniformly distributed $\mu_i, \mu_i' \in_R [-\frac{1}{2}, \frac{1}{2}]$ we have the following mean values :* 1. $\mathcal{E}[|\mu_i|^2] = \frac{1}{12}$, 2. $\mathcal{E}[|\mu_i|] = \frac{1}{4}$.

Proof. 1. $\mathcal{E}[|\mu_i|^2] = 2\int_0^{\frac{1}{2}} x^2 \mathrm{dx} = \frac{1}{12}$, 2. $\mathcal{E}[|\mu_i|] = 2\int_0^{\frac{1}{2}} x\,\mathrm{dx} = \frac{1}{4}$. □

The Geometric Series Asumption (GSA). We assume that the $\|\widehat{b}_i\|^2$ form a geometric series, $\|\widehat{b}_i\|^2 = \|b_1\|^2 q^{i-1}$ for $i = 1, ..., n$ with some quotient $q < 1$.

Justification of the GSA. We merely use the GSA to simplify the analysis. Typically, the GSA holds in an approximate way — $\|\widehat{b}_i\|^2 \sim \|b_1\|^2 q^{i-1}$ — if the basis has been reduced in a primal/dual way.
Moreover, the GS–property means that the lattice basis has the following worst case property

$$\|b_1\|/\|\widehat{b}_n\| = \max_{1\le i<j\le n} (\|\widehat{b}_i\|/\|\widehat{b}_j\|)^{(n-1)/(j-i)} = q^{-(n-1)/2}.$$

If GSA does not hold there exists $1 \le i < j \le n$ such that

$$\|\widehat{b}_i\|/\|\widehat{b}_j\| > (\|\widehat{b}_1\|/\|\widehat{b}_n\|)^{(j-i)/(n-1)}$$

and $j-i < n-1$. Then it suffices to reduce the subbasis $\pi_i(b_i), \ldots, \pi_i(b_j)$, where π_i is the orthogonal projection into $\mathrm{span}(b_1, \ldots, b_{i-1})^{\perp}$. Reducing that subbasis of dimension $j-i+1$ is an easier problem as its dimension $j-i+1$ is smaller than n. Such a low dimensional approach is excluded under the GSA.

Sampling Short Vectors. Let $k, k' \ge 1$ be constants, $k+k' < n$. Consider the event that a sampled vector $b = \sum_{i=1}^{n} \mu_i \widehat{b}_i$ satisfies

$$|\mu_i| \le \tfrac{1}{2} \cdot q^{(k-i)/2} \qquad \text{for } \ i = 1, ..., k. \tag{3}$$

Under RA that event has probability

$$\prod_{i=1}^{k} q^{(k-i)/2} = q^{\binom{k}{2}/2} = q^{k(k-1)/4}.$$

We study the probability that $\|b\|^2 < \|b_1\|^2$ holds under RA and the conditions (1), (3).

Lemma 2. SAL *samples vectors* b *that satisfy under* GSA *and* RA *that* $\Pr[\,\|b\|^2\,\|b_1\|^{-2} \le \frac{1}{12}[k\,q^{k-1}+(q^k+3\,q^{n-k'}-4q^n)/(1-q)] \ge \frac{1}{2}q^{-k(k-1)/4}$.

Proof. By Lemma 1 we have under (1), (3) the mean value

$$\mathcal{E}[\,|\mu_i|^2\,|\,(3)\,] \;=\; \begin{cases} \frac{1}{12}\,q^{k-i} & \text{for } i=1,\ldots,k \\ 1/12 & \text{for } i=k+1,...,n-k' \\ 1/3 & \text{for } i=n-k'+1,\ldots,n-1 \end{cases}.$$

Under GSA this yields $\mathcal{E}[\,\|b\|^2\|b_1\|^{-2}\;|\;(3)\,]$

$$\le \tfrac{1}{12}\Big[\textstyle\sum_{i=1}^{k} q^{k-i}\|\widehat{b}_i\|^2 + \sum_{i=k+1}^{n-k'}\|\widehat{b}_i\|^2 + 4\sum_{i=n-k'+1}^{n}\|\widehat{b}_i\|^2\Big]$$

$$= \tfrac{1}{12}\Big[\textstyle\sum_{i=1}^{k} q^{k-i+i-1} + q^k\sum_{i=1}^{n-k-k'} q^{i-1} + 4\,q^{n-k'}\sum_{i=1}^{k'} q^{i-1}\Big]$$

$$= \tfrac{1}{12}\Big[k\,q^{k-1} + q^k(1-q^{n-k-k'}) + 4q^{n-k'}(1-q^{k'}))/(1-q)\Big]$$

$$= \tfrac{1}{12}\,[k\,q^{k-1} + (q^k + 3\,q^{n-k'} - 4\,q^n)/(1-q)].$$

Now the claim follows as (3) holds with probability $q^{k(k-1)/4}$. □

Theorem 1. *Let* $k \ge 32$ *and* $n \ge 2k + \frac{k}{4\ln 2}\ln(k/6)$. *There is an algorithm which runs under* GSA *and* RA *in average time* $O(n^3(k/6)^{k/4}+n^4)$ *and which transforms a given* LLL*-reduced basis into a basis with an approximation factor less than* $(k/6)^{n/2k}$. [2]

Proof. The algorithm performs the following steps.

1. Sample distinct lattice vectors b via SAL until $\|b\|^2 < \|b_1\|^2$, where $k' = \frac{k}{4\ln 2}\ln(k/6)$ in SAL.
2. Extend the short vector b to an LLL-reduced basis with $b_1 = b$. This is done by one LLL-type reduction. This LLL-type reduction requires not more than $O(n^3)$ steps because it remodels a given LLL-reduced lattice basis.
3. If $\|b_1\|/\|\widehat{b}_n\| \le (k/4)^{(n-1)/(2k)}$ then terminate and output the basis. Otherwise go to 1 and iterate the algorithm.

Analysis. We apply Lemma 2 to the geometric series $\|\widehat{b}_i\|^2 = \|b_1\|^2 q^{1-i}$ of the lattice basis given in Step 1. We show that $\frac{1}{12}\,[k\,q^{k-1} + (q^k + 3\,q^{n-k'} - 4\,q^n)/(1-q)] < 1$ holds for $q = 1 - \frac{\ln(k/6)}{k}$. If q is smaller then SAL succeeds even better. We have that

$$\tfrac{k}{12}q^k \le \tfrac{k}{12}(1-\tfrac{\ln(k/6)}{k})^k < \tfrac{k}{12}e^{-\ln(k/6)} = \tfrac{k}{12}\tfrac{6}{k} = \tfrac{1}{2}.$$

We get from $\frac{k}{12}q^k < \frac{1}{2}$ and $n - k' \ge 2k$ that

$$\tfrac{1}{12}\,(q^k + 3q^{n-k'} - 4q^n)/(1-q) \le \tfrac{1}{12}\,q^k\,\tfrac{k}{\ln(k/6)}(1+3/k) < \tfrac{1}{2}\,\tfrac{1+3/k}{\ln(k/6)}.$$

Hence $\frac{1}{12}\,[k\,q^{k-1}+(q^k+3\,q^{n-k'}-4\,q^n)/(1-q)] \le \frac{1}{2}(\frac{1+3/k}{\ln(k/6)}+1/q) < 0.94$, as $\frac{1+3/k}{\ln(k/6)} + 1/q < 2\cdot 0.94$ holds for $k \ge 32$ and $q = 1 - \frac{\ln(k/6)}{k}$.

[2] We let ln denote the natural logarithm with base $e \approx 2.718$.

Lemma 2 shows that $\|b\|^2\|b_1\|^{-2} < 0.94$ holds at least with probability $\frac{1}{2}\,q^{k(k-1)/4}$, where

$$q^{k(k-1)/4} = (1 - \tfrac{\ln(k/6)}{k})^{k(k-1)/4} > e^{-(k-1)\ln(k/6)/4} = (k/6)^{(-k+1)/4}.$$

Hence $\Pr[\|b\|^2 < 0.94\,\|b_1\|^2] > \frac{1}{2}(k/6)^{(-k+1)/4}$.

Therefore SAL suceeds with a short b in average time $O(n^2(k/6)^{(k-1)/4})$. The algorithm performs at most $O(n)$ iterations, an iteration requires $O(n^2(k/6)^{k/4})$ steps for SAL and $O(n^3)$ steps for the LLL-reduction. Therefore the entire algorithm runs in average time $O(n^3(k/6)^{k/4} + n^4)$. Upon termination we have that $q > 1 - \frac{\ln(k/6)}{k}$. The resulting approximation factor is bounded by

$$q^{-n/2} < (1 - \tfrac{\ln(k/6)}{k})^{\frac{-k}{\ln(k/6)}\frac{n}{k}\frac{\ln(k/6)}{2}} < e^{\frac{n}{k}\frac{\ln(k/6)}{2}} = (k/6)^{\frac{n}{2k}}.$$

We need that $2^{k'} \geq q^{-k(k-1)/4}$ so that enough vectors can be sampled. It is sufficient that $k' \geq \frac{k^2}{4}\log_2(1/q) \approx \frac{k}{4\ln 2}\ln(k/6)$. □

Remark. We can replace in Theorem 1 the fraction $(k/6)$ by $k/(12-\varepsilon)$ for an arbitrary $\varepsilon > 0$, provided that k is sufficiently large, i.e., $k \geq k_0(\varepsilon)$. This follows from $\frac{12-\varepsilon}{12}\,\frac{1}{\ln(k/12)} = o(1)$ for sufficiently large k.

Refined Analysis. While the inequalities (3) are sufficient to make $\|b\|^2\|b_1\|^{-2}$ small they are not necessary. We show that $\Pr[\|b\|^2\|b_1\|^{-2} < 1] \geq \frac{1}{2}e^{k/8}q^{k(k-1)/4}$ for $q = 1 - \frac{\ln(k/6)}{k}$, thus increasing the probability that SAL generates a short vector by the factor $e^{k/8}$.
We liberalize the Inequalities (3) by allowing a few larger coefficiens $|\mu_i|$. We balance the larger values $|\mu_i|$ by requiring that the remaining $|\mu_i|$ are even smaller than $\frac{1}{2}q^{(k-i)/2}$ so that $\sum_{i=1}^{k}|\mu_i|^2\|\widehat{b}_i\|^2 \leq k\,q^{k-1}$ as before. We allow $k/4$ larger coefficients $|\mu_{j_i}|$ satisfying

$$\tfrac{1}{2}\,q^{(k-j_i)/2} < |\mu_{j_i}| \leq q^{(k-j_i)/2} \qquad \text{for } 1 \leq j_i \leq k/2,\ i = 1, ..., k/4.$$

(we require that $j_i \leq k/2$ so that $q^{(k-j_i)/2} \leq \frac{1}{2}$.) These larger $|\mu_{j_i}|$ can be balanced by requiring that

$$|\mu_i| \leq \tfrac{1}{2}\,q^{(k-i)/2}(1 - \tfrac{1}{k})^{k/4} \qquad \text{for } i \notin \{j_1, ..., j_{k/4}\},\ 1 \leq i \leq k.$$

For a constant selection of $j_1, ..., j_{k/4}$ the modified inequalities (3) imply under RA that

$$\mathcal{E}[\textstyle\sum_{i=1}^{k}|\mu_i|^2\|\widehat{b}_i\|^2] = \frac{1}{12}q^{k-1}[1 + O(\frac{1}{k})].$$

Moreover, these inequalities hold with probability $q^{k(k-1)/4}(1-\frac{1}{k})^{k/4(k-k/4)} \approx q^{k(k-1)/4}e^{-3k/4}$. The number of choices for the $k/4$ values $j_1, ..., j_{k/4}$ is $\binom{\frac{k}{2}-1}{k/4} \geq e^{k/8}$. Different choices correspond to disjoint events so that

the probabilities add up. This yields $\Pr[\sum_{i=1}^{k} |\mu_i|^2 \|\widehat{b}_i\|^2 \leq \frac{1}{2}\, k q^{k-1}] \geq \frac{1}{2} e^{k/8} q^{k(k-1)/4}$. For $k' = 31,\ n \geq 160$ we get the following performance values:

k	q	time	proven approx. factor
54	0.963	$n^3 2^{31}$	1.019^n
40	0.957	$n^3 2^{19}$	1.022^n
30	0.950	$n^3 2^{13}$	1.026^n
24	0.946	$n^3 2^8$	1.028^n
20	0.942	$n^3 2^7$	1.03^n
11	0.93	$n^3 2^3$	1.037^n

For example, we have for $k = 54$, $k' = 31$, $n \geq 160$, $q = 0.963$ that

$$\mathcal{E}[\, \|b\|^2 \, \|b_1\|^{-2} \mid (3)\,] = \tfrac{1}{12}[k\, q^{k-1} + \tfrac{q^k + 3\, q^{n-k'} - 4q^n}{1-q}] < 0.94.$$

As (3) holds with probability $q^{k(k-1)/4} \approx 1.06 \cdot 2^{-39}$ this yields

$$\Pr[\, \|b\|^2 \leq 0.94\, \|b_1\|^2] \geq \tfrac{1}{2}\, e^{54/8} q^{k(k-1)/4} \geq 1.77 \cdot 2^{-31}.$$

Therefore, the algorithm of Theorem 1 yields the quotient $q > 0.963$. Such q corresponds to an approximation factor $q^{-(n-1)/2} < 1.019^{n-1}$. In the cases of $k = 40, 30, 25, 20, 11$ we proceed accordingly.

Birthday Sampling. The birthday paradox is a well known heuristic that reduces the number of vectors to be sampled to its square root. Instead of searching for a lattice vector b with $\|b\| < \|b_1\|$ we sample distinct vectors until two vectors b, b' arise with $\|b - b'\| < \|b_1\|$. We study the probability that $\|b - b'\|^2 \|b_1\|^{-2} < 1$ for distinct vectors b, b' generated by SAL. We assume in addition to RA that the coefficients μ_i of b and μ_i' of b' are statistically independent.

Lemma 3. *Let $\mu_i, \mu_i' \in_R [-\frac{1}{2}, \frac{1}{2}]$ be uniformly distributed and statistically independent. Then we have the following mean values :*
1. $\mathcal{E}[|\mu_i \pm \mu_i'|^2] = \frac{1}{6}$ *for either sign* $\pm$, 2. $\mathcal{E}[|\mu_i - \mu_i'|] = \frac{3}{8}$.

Proof. 1. $\mathcal{E}[|\mu_i \pm \mu_i'|^2] = \int_{-\frac{1}{2}}^{\frac{1}{2}} \int_{-\frac{1}{2}}^{\frac{1}{2}} x^2 + y^2 \pm 2xy \,\mathrm{dx}\,\mathrm{dy} =$

$\int_{-\frac{1}{2}}^{\frac{1}{2}} [x^3/3 + x\, y^2 \pm x^2 y]\Big|_{-\frac{1}{2}}^{\frac{1}{2}} \mathrm{dy} = \frac{1}{12} + \int_{-\frac{1}{2}}^{\frac{1}{2}} y^2 \,\mathrm{dy} = \frac{1}{12} + \frac{1}{12} = \frac{1}{6}.$

2. We have that $\mathcal{E}[\mu_i - \mu_i' \mid \mu_i \leq 0 \leq \mu_i'] = 2 \int_0^{\frac{1}{2}} (\frac{1}{4} + x)\mathrm{dx} = \frac{1}{2}$. With probability $\frac{1}{2}$ we either have $\mu_i \leq 0 \leq \mu_i'$ or $\mu_i' \leq 0 \leq \mu_i$. Also with probability $\frac{1}{2}$ we either have $\mu_i, \mu_i' \leq 0$ or $\mu_i', \mu_i \geq 0$. We infer that $\mathcal{E}[|\mu_i - \mu_i'|] = \frac{1}{2} \cdot \frac{1}{2} + \frac{1}{2} \cdot \mathcal{E}[\frac{1}{2}|\mu_i - \mu_i'|] = \frac{1}{4} + \frac{1}{8} = \frac{3}{8}$. □

Lemma 4. *Distinct vectors b, b' sampled via* SAL *satisfy under* RA *that* $\Pr\Big[\, \|b-b'\|^2 \|b_1\|^{-2} \le \frac{1}{6}\,[kq^{k-1} + (q^k + 3q^{n-k'} - 4q^n)/(1-q)]\Big] \ge \frac{1}{2}\, q^{\binom{k}{2}/2}$.

Proof. We proceed as in the proof of Lemma 2. However, we use that $\mathcal{E}[|\mu_i \pm \mu_i'|^2] = \frac{1}{6} = 2\,\mathcal{E}[\,|\mu_i|^2]$ due to Lemma 1 and 4.
Consider the event that two vectors $b = \sum_{i=1}^n \mu_i \widehat{b}_i$, $b' = \sum_{i=1}^n \mu_i' \widehat{b}_i$ sampled by SAL satisfy

$$\textstyle\sum_{i=1}^k |\mu_i - \mu_i'|^2 q^{i-1} \le \frac{1}{6} k q^{k-1}. \qquad (3^*)$$

By Lemma 3, the probability of the event (3^*) is at least $q^{\binom{k}{2}/2}$ under RA. Moreover,
$\Pr\Big[\, \|b-b'\|^2 \|b_1\|^{-2} \le \frac{1}{6}\,[kq^{k-1} + (q^k + 3q^{n-k'} - 4q^n)/(1-q)] \,|\, (3^*)\Big] \ge \frac{1}{2}$.
Hence the claim. □

Theorem 2. *Let $k \ge 32$ and $n \ge 2k + \frac{k}{2\ln 2}\ln(k/3)$. There is an algorithm which runs under* GSA *and* RA *in average time $O(n^3(k/3)^{k/8} + n^4)$ and which transforms a given* LLL*-reduced basis into a basis with an approximation factor less than $(k/3)^{n/2k}$.*

Sketch of Proof. Proceed as in the proof of Theorem 1. However, set $q := 1 - \frac{\ln(k/3)}{k}$ to offset the additional factor 2 from $\mathcal{E}[|\mu_i \pm \mu_i'|^2] = 2\,\mathcal{E}[\,|\mu_i|^2]$. Generate $O(n(k/3)^{k/8})$ lattice vectors b via SAL and search for short vectors $b-b'$ so that (3^*) holds. Such vectors $b-b'$ can be found efficiently. This algorithm needs to store $O(n(k/3)^{k/8})$ lattice vectors. □

Theorem 2 shows that birthday sampling is for large values k superior to random sampling. The crossover point, where birthday sampling gets more efficient, is for a large k. Birthday sampling is more efficient for $q = 0.98$, $k = 175$ with an $n^3 2^{80}$-time algorithm.

3 Towards a Practical Sieve Algorithm

The Goal of the Sieve. Our method is inspired by Aijtai, Kumar, Sivakumar [AKS01]. Consider a lattice basis $b_1, \ldots, b_n \in \mathbf{Z}^n$ of dimension n with orthogonalization vectors $\widehat{b}_1, \ldots, \widehat{b}_n$. Let k be some integer $1 < k < n$, $k = 4^t$, throughout the following k will be a power of 4. We present a novel, efficient deterministic algorithm that transforms an LLL-reduced basis into a basis satisfying

$$\textstyle\sum_{i=k+1}^n \|\widehat{b}_i\|^2 \;>\; \frac{1}{4k}\;\|b_1\|^2. \qquad (4)$$

We bound in Lemma 5 the *approximation factor* $\|b_1\|/\lambda_1$ for lattice bases having property (4). Our time bounds count arithmetic steps using integers bounded by $\max_i \|b_i\|^2$.

The Basic Sieve. Suppose we are given an LLL–reduced lattice basis satisfying $\sum_{i=k+1}^{n} \|\widehat{b}_i\|^2 \leq \frac{1}{4k} \|b_1\|^2$ for some k such that $3k+1 \leq n$. We proceed in t stages, $s = 0, ..., t-1$. Initially, at stage 0 we generate 2^{2k+1} lattice vectors $b = \sum_{i=1}^{n} t_i b_i = \sum_{i=1}^{n} \mu_i \widehat{b}_i$ satisfying

$$|\mu_i| \leq \begin{cases} \frac{1}{2} \text{ for } i \leq k \\ 1 \text{ for } k < i < n \end{cases}, \qquad \mu_n \in \{1, 2\}. \tag{5}$$

There are at least 2^{n-k} distinct lattice vectors b of this form. We let $n \geq 3k+1$ so that there are 2^{2k+1} vectors for stage 0. The vectors of stage 0 are *positive* , i.e., $\mu_i > 0$ for the largest i with $\mu_i \neq 0$ and $b \neq \mathbf{0}$. A vector b of stage 0 can easily be generated in time $O(n^2)$, which yields the time bound $O(n^2 2^{2k+1})$ for stage $s = 0$. Stage $s \geq 1$ requires only $O(n 2^{2k+1})$ steps. As the number of stages t is small compared to n the total time for the sieve is essentially the time for stage 0.

Stage $s \geqq 1$. By induction on s we generate 2^{2k+1} positive vectors $b = \sum_{i=1}^{n} \mu_i \widehat{b}_i$ of stage s satisfying

$$|\mu_i| \leq 2^{-s-1} \quad \text{for } i \leq k, \tag{6}$$

$$|\mu_i| \leq 2^{s} \quad \text{for } k < i < n, \quad 0 \leq \mu_n \leq 2^{s-1}. \tag{7}$$

We partition the vectors b of stage s into 2^{2k} classes. We divide the range $]-1, 1] \cdot 2^{-s-1}$ of the μ_i for $i \leq k$ into 4 intervals $]j, j+1] \cdot 2^{-s-2}$ of equal size for $j = -2, -1, 0, 1$. A class is given by $j_i \in \{-2, -1, 0, 1\}$ for $i = 1, \ldots, k$ and consists of the vectors $b = \sum_{i=1}^{n} \mu_i \widehat{b}_i$ satisfying

$$\mu_i \in]j_i, j_i + 1] \cdot 2^{-s-2} \quad \text{for } i = 1, \ldots, k.$$

The vectors of stage $s+1$ are positive vectors $b \mp b'$, where b, b' are vectors of stage s, $b \neq \pm b'$ such that $b, \pm b'$ are in the same class. As there are 2^{2k} classes, the 2^{2k+2} vectors $\pm b$ of stage $s$generate at least $2^{2k+2} - 2^{2k}$ *collision pairs* $(b, \pm b')$, where $b, \pm b'$ fall into the same class and $b \mp b'$ is positive. These collisions provide at least $2^{2k}(4-1)$ vectors $b \mp b'$ for stage $s+1$ counted with multiplicities, and satisfying $b \mp b' = \sum_{i=1}^{n} (\mu_i \mp \mu_i') \widehat{b}_i$ such that $|\mu_i \mp \mu_i'| \leq 2^{-s-2}$ for $i = 1, \ldots, k$. This shows the induction claim for (3) while the induction for (4) is trivial. In particular, we have that $0 \leq \mu_n \leq 2^{s-1}$ as $\mu_n \in \{1, 2\}$ for stage 0. We keep from all possible vectors $b \mp b'$ of stage $s+1$ at most 2^{2k+1} distinct, positive vectors, we discard repetitions of the same vector.

The number of distinct vectors of stage $s+1$ is at least $2^{2k}(4-1)$ minus the number of *repetitions*, where $b - b' = \overline{b} - \overline{b}'$ holds for two collision pairs $(b, b'), (\overline{b}, \overline{b}')$. We make the heuristic

Few Repetitions Assumption (FRA). We assume that the number of repetitions at stage s is not greater than the number of classes.

Under the FRA there are for each stage s at least $2^{2k}(4-2) = 2^{2k+1}$ distinct, non-zero vectors. We will see that all vectors b of stage t satisfy

$\|b\|^2 \leq \frac{1}{2}\|b_1\|^2$. Therefore, the FRA requires that there are plenty of lattice vectors b satisfying $\|b\|^2 \leq \frac{1}{2}\|b_1\|^2$. Conversely, we justify below the FRA for the case that $\|b_1\| \geq n \cdot \|\widehat{b}_n\|$.

At the final stage $t := \frac{1}{2}\log_2 k$ we have that

$$|\mu_i|^2 \;\leq\; \begin{cases} 2^{-2t-2} = \frac{1}{4k} & \text{for } \; i \leq k \\ 2^{2t} \;\; = \;\; k & \text{for } \; i > k \end{cases} .$$

Using that (4) is violated and $\|b_1\| = \max_{i \leq k} \|\widehat{b}_i\|$ we have that

$$\textstyle\sum_{i=1}^n |\mu_i|^2 \|\widehat{b}_i\|^2 \|b_1\|^{-2} \leq \sum_{i=1}^k |\mu_i|^2 + k \sum_{i=k+1}^n \|\widehat{b}_i\|^2 \|b_1\|^{-2} \leq \frac{1}{4} + \frac{1}{4}.$$

This shows that the vectors b of stage t satisfy $\|b\|^2 \leq \frac{1}{2}\|b_1\|^2$, hence:

Theorem 3. *Given a lattice basis satisfying* $\sum_{i=k+1}^n \|\widehat{b}_i\|^2 \leq \frac{1}{4k}\|b_1\|^2$ *for* $n \geq 3k+1$ *the basic sieve finds in deterministic time* $O(n^2 2^{2k+1})$ *under* FRA 2^{2k+1} *distinct lattice vectors* b*, all satisfying* $\|b\|^2 \leq \frac{1}{2}\|b_1\|^2$.

Suppose we are given an LLL-reduced basis satisfying $\|b_1\|^2 \leq 2^n \lambda_1^2$. Then we can halve $\|b_1\|^2$ at most n times. Iterating the basic sieve at most n times we get a basis satisfying (4). The time bound for this procedure is $O(n^3 2^{2k+1})$.

Assuming the GSA. In order to interpret property (4) in terms of the approximation factor $\|b_1\|/\lambda_1$ we assume that the $\|\widehat{b}_i\|^2$ form a geometric series, $\|\widehat{b}_i\|^2 = \|b_1\|^2 q^{i-1}$ for $i = 1, ..., n$ with some quotient $q < 1$.

Lemma 5. *For* $1 \leq \alpha < k/\ln k, 1 < k < n$*, a geometric series* $\|\widehat{b}_i\|^2$ *with quotient* $q = 1 - \frac{\alpha \ln k}{k}$ *satisfies* $\sum_{i=k+1}^n \|\widehat{b}_i\|^2 \|b_1\|^{-2} \leq 1/(\alpha k^{\alpha-1} \ln k)$.

Proof. We have that

$$\begin{aligned} \textstyle\sum_{i=k+1}^n \|\widehat{b}_i\|^2 \|b_1\|^{-2} \;&=\; \tfrac{q^k - q^n}{1-q} \\ <\; q^k/(1-q) \;&=\; (1 - \tfrac{\alpha \ln k}{k})^k \tfrac{k}{\alpha \ln k} \\ <\; e^{-\alpha \ln k} \tfrac{k}{\alpha \ln k} \;&=\; 1/(\alpha k^{\alpha-1} \ln k) \;, \end{aligned}$$

where we use that $(1 - \frac{1}{k})^k < e^{-1}$. □

Corollary 1. *A lattice basis satisfying* (4) *has under the* GSA *an approximation less than factor* $(k+\varepsilon)^{n/k}$*,* $\varepsilon = O(k^{-2} \ln k)$.

Proof. A geometric series $\|\widehat{b}_i\|^2$ satisfying (4) has by Lemma 5 a quotient $q \geq 1 - \frac{2 \ln k}{k}$ provided that $\ln k \geq 2$. Hence

$$\begin{aligned} &\|b_1\|/\lambda_1 \leq \|b_1\|/\|\widehat{b}_n\| = q^{-n/2} \leq (1 - \tfrac{2 \ln k}{k})^{-n/2} \\ =\; &(e + O(k^{-2}))^{(n/k) \ln k} \;=\; (k + O(k^{-2} \ln k))^{n/k}. \end{aligned}$$

□

The Tailored Sieve. Instead of distributing the μ_i to 4 subintervals for every $i \leq k$ we adjust the number of subintervals to the length of $\widehat{b}_i$. We need more subintervals for μ_i over all stages the longer $\widehat{b}_i$, so that upon termination we have that $|\mu_i|^2\|\widehat{b}_i\|^2 \leq \frac{1}{4k}$. As we need no subintervals for $i > k$ and only a few intervals for the i near to k we can save about half of the intervals for the average i, and thus reduce the number of classes per stage from 2^{2k} to 2^k.

We outline the construction, we tailor the sieve assuming for simplicity the GSA. Let a given lattice basis satisfy $\sum_{i=k+1}^{n} \|\widehat{b}_i\|^2 \leq \frac{1}{4k}\|b_1\|^2$. Lemma 3 with $\alpha = 2$, $k > e^2$ shows that $q < 1 - \frac{\alpha \ln k}{k}$ and thus

$$\|\widehat{b}_i\|^2/\|b_1\|^2 = q^{i-1} < k^{-\alpha\frac{i-1}{k}}.$$

We let $n \geq 2k+1$ so that there are 2^{k+1} vectors $b = \sum_{i=1}^{n} \mu_i \widehat{b}_i$ with $|\mu_i| \leq 1$ for $i = k+1, ..., n-1$, $\mu_n \in \{1, 2\}$. We tailor the sieve so that the μ_i of stage s range over an interval $]-\frac{1}{2}, \frac{1}{2}] \cdot 2^{\eta_{i,s}}$ where the integers $\eta_{i,s}$ are recursively defined so that

$$\begin{aligned} &\eta_{i,0} = 0 \quad \text{and} \quad \eta_{i,s+1} - \eta_{i,s} \in \{-1, 0, 1\} \quad \text{for} \quad i = 1, \ldots, k \\ &\eta_{i,s} = s + 1 \qquad \text{for} \quad i = k+1, \ldots, n. \end{aligned}$$

Upon termination at stage $t = \frac{1}{2}\log_2 k$, we want to have that

$$2^{2\eta_{i,t}} \leq k^{-1+\alpha\frac{i-1}{k}} \quad \text{for } i \leq k$$

which implies that $\sum_{i=1}^{k} |\mu_i|^2\|\widehat{b}_i\|^2\|b_1\|^{-2} \leq \frac{k}{4k} = \frac{1}{4}$.

At stage s we partition the range $]-\frac{1}{2}, \frac{1}{2}] \cdot 2^{\eta_{i,s}}$ of the μ_i into $2^{\nu_{i,s}}$ intervals of equal length where $\nu_{i,s}$ is either $0, 1, 2$. Then the vectors $b \mp b'$ of stage $s+1$ with $b, \pm b'$ in the same class satisfy $\mu_i \mp \mu_i' \in]-\frac{1}{2}, \frac{1}{2}] \cdot 2^{\eta_{i,s} - \nu_{i,s}+1}$. We see that $\eta_{i,s+1} = \eta_{i,s} - \nu_{i,s} + 1$, and thus $\eta_{i,t} = t - \sum_{s=0}^{t-1} \nu_{i,s}$.

We select the $\nu_{i,s}$ as to minimize the number $2^{\sum_i \nu_{i,s}}$ of equivalence classes of stage s. The $\nu_{i,s}$ must satisfy for $i = 1, ..., k$

$$\sum_{s=0}^{t-1} \nu_{i,s} \geq 2t - \alpha\, t\frac{i-1}{k} \tag{8}$$

so that $2^{2\eta_{i,t}} \leq 2^{-2t+2\alpha\, t\frac{i-1}{k}} \leq k^{-1+\alpha\frac{i-1}{k}}$ holds upon termination for $t = \frac{1}{2}\log_2 k$. To meet Inequality (8) for the average i we select the $\nu_{i,j}$ such that $\sum_{s=0}^{t-1} \nu_{i,s} = \lceil 2t - \alpha t\frac{i-1}{k} \rfloor$, where $\lceil r \rfloor$ denotes the nearest integer to r. Moreover, we balance the sums $\sum_i \nu_{i,s}$ so that two sums for different stages differ at most by 1. We see from $\sum_{i=1}^{k} \lceil 2t - \alpha t\frac{i-1}{k} \rfloor \approx 2tk - tk$ for $\alpha = 2$ that $\sum_{i=1}^{k} \nu_{i,s} \leq k+1$. Then there are $2^{\sum_i \nu_{i,s}} \leq 2^{k+1}$ classes per stage. Therefore it suffices to generate 2^{k+1} vectors per stage which yields a time bound $O(n^2 2^{k+1})$ for the sieve. This proves the following

Theorem 4. *Given a lattice basis satisfying* $\sum_{i=k+1}^{n} \|\widehat{b}_i\|^2 \leq \frac{1}{4k}\|b_1\|^2$, *for* $n \geq 2k + o(k)$, *the tailored sieve finds in average time* $O(n^2 2^{k+1})$ *under* FRA *and* GSA 2^k *lattice vectors* b *all satisfying* $\|b\|^2 \leq \frac{1}{2}\|b_1\|^2$.

Iteration of the taylored sieve yields for $k \approx \frac{n}{2}$ by Theorem 4 and Corollary 1 the approximation factor $\approx k^{\frac{n}{k}} = (\frac{n}{2})^2$ in time $O(2^{\frac{n}{2}+o(n)})$.

How to Justify FRA *under* GSA *for the Taylored Sieve.* The GAUSSIAN volume heuristics tells us that the number of lattice points b such that $\|b\|^2 \leq \frac{1}{2}\|b_1\|^2$ is on average

$$\frac{V_n(\|b_1\|/\sqrt{2})}{\|\widehat{b}_1\| \cdot ... \cdot \|\widehat{b}_n\|} = \frac{2^{-n/2}\|b_1\|^n}{\Gamma(\frac{n}{2}+1) \cdot \|\widehat{b}_1\| \cdot ... \cdot \|\widehat{b}_n\|} \approx \Big(\frac{2e\pi}{n}\Big)^{2\,\frac{n}{2}} \frac{\|b_1\|^n}{\|\widehat{b}_1\| \cdot ... \cdot \|\widehat{b}_n\|},$$

where $V_n(r)$ is the volume of the n-dimensional sphere with radius r. Under the GSA we have that

$$\prod_{i=1}^{n} \|b_1\|/\|\widehat{b}_i\| = \prod_{i=1}^{n} \Big(\|b_1\|/\|\widehat{b}_n\|\Big)^{\frac{i-1}{n-1}} = \Big(\|b_1\|/\|\widehat{b}_n\|\Big)^{\frac{n}{2}}.$$

Thus the number of lattice points b such that $\|b\|^2 \leq \frac{1}{2}\|b_1\|^2$ is on average

$$\approx \Big(\tfrac{e\pi\|b_1\|}{n\cdot\|\widehat{b}_n\|}\Big)^{\frac{n}{2}} \geq (e\pi)^{\frac{n}{2}} \approx 2.92^n,$$

provided that $\|b_1\| \geq n \cdot \|\widehat{b}_n\|$. Thus the number of lattice points b such that $\|b\|^2 \leq \frac{1}{2}\|b_1\|^2$ is much larger than the number 2^{k+1}, required for the taylored sieve. This justifies the FRA for the taylored sieve in the case that $\|b_1\| \geq n \cdot \|\widehat{b}_n\|$.

The Approximation Factor n. Theorem 4 requires that $k < \frac{n}{2}$. Now we remove this conditions that is used to provide enough vectors for stage 0 of the taylored sieve. This yields under FRA and GSA the approximation factor n within average time $O(2^{n+o(n)})$.

Theorem 5. *There is an algorithm that transforms under* FRA *and* GSA *an* LLL*-reduced lattice basis of dimension $n = 4^t + 1$ in determinisitic time $2^{n+o(n)}$ into a basis satisfying $\|b_1\| \leq n\,\|\widehat{b}_n\|$.*

Proof. We proceed as in the taylored sieve for $k = n-1$, $\alpha = 2$, $t = \frac{1}{2}\log_2 k$. However, we allow for the vectors of stage 0 that $|\mu_i| \leq \frac{1}{2}\cdot 2^{1+\delta_i}$ for $i = 1, ..., n-1$, $\mu_n \in \{1, 2\}$. We let the integers δ_i satisfy $2n/t + 1 \leq \sum_i \delta_i < n$ so that we get at least $2^{n+2n/t+1}$ vectors for stage 0. We compensate for the larger $|\mu_i|$, $|\mu_i| > \frac{1}{2}$, by additionally halving these $|\mu_i|$ via the sieve $1+\delta_i$-times over the t stages. This increases the number of classes per stage by the factor $2^{(n+\sum_i \delta_i)/t} < 2^{2n/t}$ from 2^n to at most $2^{n+2n/t}$. Thus, the number of classes per stage, the number of vectors per stage and the time are all boundedby $2^{n+o(n)}$.

The final vectors vectors $b = \sum_{i=1}^{n} \mu_i \widehat{b}_i$ at stage $t = \frac{1}{2}\log_2 k$ satisfy for $i = 1, ..., n-1$ that

$$|\mu_i| \leq \tfrac{1}{2}2^{1+\delta_i-1-\delta_i}2^{-\frac{1}{2}\log_2 k} = \tfrac{1}{2}/\sqrt{k}, \quad |\mu_n| \leq \tfrac{1}{2}2^{\frac{1}{2}\log_2 k} = \tfrac{1}{2}\sqrt{k}.$$

Hence

$$\|b\|^2 = \textstyle\sum_{i=1}^{n} |\mu_i|^2\|\widehat{b}_i\|^2 \leq \frac{1}{4}\frac{n-1}{n-1}\,\|b_1\|^2 + \frac{n-1}{4}\,\|\widehat{b}_n\|^2 < \frac{1}{2}\cdot\|b_1\|^2,$$

where we use that $\|b_1\| \geq n \cdot \|\widehat{b}_n\|$ and that $\|b_1\| = \max_i \|\widehat{b}_i\|$. □

Applying the sieve iteratively n-times to an LLL-reduced basis results in a basis satisfying $\|b_1\| \leq n \cdot \|\widehat{b}_n\|$. The property $\max_{i=1,\ldots,n} \|b_i\|/\|\widehat{b}_i\| \leq n$ implies that b_1 approximates λ_1 to within a factor n. Thus, the taylored sieve realizes by Theorem 5 and Corollary 1 the approximation factor n.

The Randomized Sieve. So far our worst case analysis uses that $|\mu_i - \mu_i'|^2 \leq \frac{1}{4}$ holds for $\mu_i, \mu_i' \in [-\frac{1}{2}, \frac{1}{2}]$. Now we give an average case analysis for random $\mu_i, \mu_i' \in_R [-\frac{1}{2}, \frac{1}{2}]$.

Randomnesss Assumption * (RA*). Let the μ_i of the vectors of stage 0 be uniformly distributed over the invervals $[-\frac{1}{2}, \frac{1}{2}]$ for $i \leq k$ resp., $[-1, 1]$ for $i > k$, and statistically independent for distinct vectors and distinct i.

We get from Lemma 1 and Lemma 4 the following

Corollary 2. *For random $\mu_i, \mu_i' \in_R [-\frac{1}{2}, \frac{1}{2}]$ we have that*

1. $\mathcal{E}[|\mu_i \pm \mu_i'|^2] = 2\,\mathcal{E}[|\mu_i|^2]$,
2. $\mathcal{E}[|\mu_i - \mu_i'|] = \frac{3}{2}\,\mathcal{E}[|\mu_i|]$.

As $\mathcal{E}[|\mu_i \pm \mu_i'|^2] = 2\mathcal{E}[|\mu_i|^2]$ it follows that

$$\mathcal{E}[\textstyle\sum_{i=k+1}^{n} |\mu_i \pm \mu_i'|^2 \|\widehat{b}_i\|^2] \;\leq 2\; \mathcal{E}[\sum_{i=k+1}^{n} |\mu_i|^2 \|\widehat{b}_i\|^2],$$

which is half the bound required for the proofs of Theorems 3 and 4. We show that Inequality (4) can be replaced by the stronger inequality

$$\sum_{i=k+1}^{n} \|\widehat{b}_i\|^2 > \tfrac{1}{4\sqrt{k}} \|b_1\|^2. \tag{4*}$$

If Inequality (4*) is violated then we have by Corollary 2 at the final stage $t = \frac{1}{2}\log_2 k$ that

$$\mathcal{E}[\sum_{i=k+1}^{n} |\mu_i|^2 \|\widehat{b}_i\|^2 \|b_1\|^{-2}] \leq 2^t \mathcal{E}[\sum_{i=k+1}^{n} \|\widehat{b}_i\|^2 \|b_1\|^{-2}] \leq \tfrac{\sqrt{k}}{4\sqrt{k}} = \tfrac{1}{4}.$$

Therefore, Inequality (4) can be replaced on the average by (4*), hence

Theorem 6. *Given a lattice basis satisfying $\sum_{i=k+1}^{n} \|\widehat{b}_i\|^2 \leq \frac{1}{4\sqrt{k}} \|b_1\|^2$ and $k < n$ the tailored, randomized sieve finds under* FRA, GSA *and* RA *$2^{k+o(k)}$ lattice vectors b all satisfying $\|b\|^2 \leq \frac{1}{2}\|b_1\|^2$.*

Corollary 3. *A lattice basis satisfying (4*) approximates under* GSA *the shortest lattice vector to within a factor $k^{\frac{3}{4}\frac{n}{k}}$.*

Proof. Replacing in (4) $\frac{1}{4k}$ by $\frac{1}{4\sqrt{k}}$ amounts by Lemma 5 under GSA to replace the quotient $q = 1 - \frac{2\ln k}{k}$ by $q = 1 - \frac{1.5\ln k}{k}$, i.e., replacing $\alpha = 2$ by $\alpha = 1.5$. By Corollary 1 a quotient $q \geq 1 - \frac{1.5\ln k}{k}$ yields an approximation factor

$$\|b_1\|/\lambda_1 \leq \|b_1\|/\|\widehat{b}_n\| = q^{-n/2}$$
$$\leq (1 - \tfrac{1.5\ln k}{k})^{-n/2} \;\approx\; e^{\frac{3}{4}\frac{n}{k}\ln k} \;=\; k^{\frac{3}{4}\frac{n}{k}}.$$

The Time Bound Under RA*. Under RA* we can tailor the sieve using smaller intervals and fewer vectors per stage. We sketch how to speed up the sieve so that there are on average $2^{0.835\,k+1}$ vectors per stage requiring a total of $O(n^2 2^{0.835\,k+o(k)})$ arithmetic steps. Suppose that the μ_i for $i \leq k$ of stage s range over the interval $]-\frac{1}{2},\frac{1}{2}]\cdot 2^{\eta_{i,s}}$. We partition that interval into $2^{\nu_{i,s}}$ subintervals of equal length. Two random μ_i, μ_i' in the same subinterval satisfy Corollary 3 on the average that

$$|\mu_i - \mu_i'| \in [-\tfrac{1}{2},\tfrac{1}{2}]\cdot 2^{\eta_{i,s}-\nu_{i,s}}\cdot\tfrac{3}{2}.$$

Hence $\eta_{i,s+1} = \eta_{i,s} - \nu_{i,s} + \log_2\frac{3}{2}$ — where $\eta_{i,s+1}$ is non-integer and $\log_2\frac{3}{2} \approx 0.585$ — and thus $\eta_{i,t} \approx 0.585\,t - \sum_s \nu_{i,s}$ for $t = \frac{1}{2}\log_2 k$. Using $\alpha = 1.5$ the worst case inequality (8) translates into an averaged inequality

$$\textstyle\sum_s \nu_{i,s} \geq 1.585\,t - \alpha t\frac{i-1}{k}. \tag{9}$$

To meet Inequality (9) for the average i we select the $\nu_{i,s}$ such that $\sum_s \nu_{i,s} = \lceil 1.585\,t - \alpha t\frac{i-1}{k}\rfloor$. Moreover we balance the sums $\sum_{i=1}^{k}\nu_{i,s}$ so that two sums for two stages s differ at most by 1. We see from $\alpha = 1.5$, $\lceil\sum_{i=1}^{k} 1.585\,t - \alpha t\frac{i-1}{k}\rfloor \approx 1.585\,kt - \frac{\alpha}{2}\,kt \approx 0.835\,kt$ that there are on average $2^{0.835\,k}$ classes per stage which yields an average time bound $O(n^2 2^{0.835\,k+1})$ for the randomized sieve.

References

[AKS01] *M. Aijtai, R. Kumar, and D. Sivakumar*, A Sieve Algorithm for the Shortest Lattice Vector Problem, Proceedings of the Thirty-Third ACM Symposium on Theory of Computing, 2001.

[H85] *B. Helfrich*, Algorithms to construct Minkowski reduced and Hermite reduced bases. *Theoretical Computer Science* **41**, pp. 125–139, 1985.

[HPS98] *J. Hoffstein, J. Pipher, and J. Silvermann*, NTRU: A new high speed public key cryptosystem, Proceedings of Algorithmic Number Theory (ANTS III), LNCS **1423**, Springer-Verlag, pp. 267–288, 1999.

[K83] *R. Kannan*, Minkowski's convex body theorem and integer programming. *Mathematics of Operations Research* **12** pp. 415–440, 1983.

[KS01a] *H. Koy and C.P. Schnorr*, Segment LLL-Reduction of Lattice Bases. Proceedings CaLC 2001, LNCS 2146, Springer-Verlag, pp. 67–80, 2001.

[KS01b] *H. Koy and C.P. Schnorr*, Segment LLL-Reduction of Lattice Bases with Floating Point Orthogonalization. Proceedings CaLC 2001, LNCS 2146, Springer-Verlag,pp. 81–96, 2001.

[KuSi] *R. Kumar and D. Sivakumar*, On polynomial approximations to the shortest lattice vector length. Proc. 12th Symposium on Discrete Algorithms, 2001,

[LLL82] *A. K. Lenstra, H. W. Lenstra, and L. Lovász*, Factoring polynomials with rational coefficients, *Math. Ann.* **261**, pp. 515–534, 1982.

[LLS90] *J.C. Lagarias, H.W. Lenstra Jr, and C.P. Schnorr*, Korkin-Zolotarev bases and successive minima of a lattice and its reciprocal lattice. *Combinatoria* **10** 4, pp. 333–348, 1990.

[S87] *C.P. Schnorr*, A hierarchy of polynomial time lattice basis reduction algorithms, *Theoretical Computer Science* **53**, pp. 201–224, 1987.

[S91] *C.P. Schnorr*, Factoring Integers and computing discrete logarithms via diophantine approximation, Proceedings os Eurocrypt'91, LNCS **547**, Springer-Verlag, pp. 281 - 293, 1991. Final paper in AMS DIMACS Series in Discr. Math. and Theor. Comp. Sc., **13**, 171 –182, 1993.