Correction to Lattice Reduction by Random Sampling and Birthday Methods

Claus Peter Schnorr
14. February 2012

We correct Table 2 of the paper that illustrates Theorem 1 by examples performance values for the algorithm SHORT under GSA and RA. We recall from the paper

Theorem 1. *Given a lattice basis $b_1, ..., b_n$ that satisfies* GSA *with quotient $q \leq (\frac{6}{k})^{1/k}$,* SHORT *runs in $O(n^2 q^{-k^2/4})$ time and finds under* RA *with probability $\frac{1}{2}$ for sufficiently large k and n a lattice vector $b \neq 0$ so that $\|b\|^2 < 0.99\,\|b_1\|^2$.*

Proof. W.l.o.g. let $q^k = \frac{6}{k}$ as the claim holds a fortiori for smaller q. The inequality

$$\tfrac{1}{12}\,[k\,q^{k-1} + (q^k + 3\,q^{n-u-1})/(1-q)] \leq \tfrac{1}{2\,q} + \tfrac{1}{12}\,\tfrac{q^k+3\,q^{3k}}{1-q} < 0.99.$$

holds for $k = 24$ and $n \geq 3k+u+1$. As $\frac{1}{2q} + \frac{1}{12}\,\frac{q^k+3\,q^{3k}}{1-q}$ decreases for $q = (\frac{6}{k})^{1/k}$ with k the inequality holds for all $k \geq 24$. Hence, the vectors b sampled by SA satisfy $\mathbf{Pr}[\,\|b\|^2\|b_1\|^{-2} < 0.99\,] \geq \frac{1}{2}\,q^{\binom{k}{2}/2}$ under GSA and RA by Lemma 2. As SHORT samples $2\,q^{-\binom{k}{2}/2}$ independent vectors b it finds with probability $1 - e^{-1} > \frac{1}{2}$ some b such that $\|b\|^2\|b_1\|^{-2} < 0.99$. □

k	q^k	$apfa = q^{\frac{-n+1}{2}}$	$\frac{\delta}{12\,q} + \frac{1}{12}\,\frac{q^k+3q^{3k}}{1-q}$	u	time
24	$6.1/k$	1.029^n	0.998	13	$n^2\,2^{12}$
32	$6.63/k$	1.0249^n	0.987	19	$n^2\,2^{18}$
40	$7/k$	1.02203^n	0.09834	24	$n^2\,2^{25}$
48	$7.3/k$	1.01985^n	0.9858	34	$n^2\,2^{33}$
56	$7.6/k$	1.018^n	0.9976	41	$n^2\,2^{40.5}$
64	$7.8/k$	1.0165^n	1.0001	50	$n^2\,2^{48.5}$
72	$7.9/k$	1.0154^n	0.9926	58	$n^2\,2^{57.6}$

Table 2. SHORT performance according to Theorem 1

For the values $\frac{\delta}{12\,q} + \frac{1}{12}\,\frac{q^k+3q^{3k}}{1-q}$ that are slightly larger than 0.99 we can achieve $\|b\|^2/\|b_1\|^2 \leq 0.99$ by letting SHORT sample more vectors b.

Table 2 gives performance values for Theorem 1 extending $q \leq (\frac{6}{k})^{1/k}$ to $q \leq (\frac{\delta}{k})^{1/k}$ for $\delta < 12$. SHORT finds in $O(n^2 q^{-k^2/4})$ time with probability $\frac{1}{2}$ for

sufficiently large k and n a nonzero lattice vector b such that $\|b\|^2 < 0.99\,\|b_1\|^2$ if

$$\tfrac{1}{12}\,[k\,q^{k-1} + (q^k + 3\,q^{n-u-1})/(1-q)] \leq \tfrac{\delta}{12\,q} + \tfrac{1}{12}\,\tfrac{q^k + 3\,q^{3k}}{1-q} < 0.99.$$

holds for $n \geq 3k + u + 1$. We used that $\frac{q^k}{1-q} = \frac{\delta(k-o(k))}{k-\delta}$ holds for $q^k = \frac{\delta}{k}$ and $k \to \infty$. Here the paper wrongly sets $\frac{\delta}{12\,q} := \frac{1}{2\,q}$ which is correct for $q^k = \frac{6}{k}$ and $k = 24$. We correct and extend this in Table 2. The correction slightly increases the approximation factor $apfa$ that bounds $\|b\|/\lambda_1$ for the lattice vector b that is found by iterating SHORT.

The achievable Hermite factor. For a basis B that satisfies GSA with quotient q we have that $\|b_1\| = q^{\frac{-n+1}{4}}\,\det(B^tB)^{\frac{1}{2n}}$, thus B has Hermite factor $q^{\frac{-n+1}{4}}$. Table 2 shows for $k = 64, 72$ that an Hermite factor $1.00822^n \approx 1.0165^{n/2}$ can be provably achieved under RA for bases with GSA. This compares well with the results of Gama and Nguyen on page 38 of Eurocrypt 2008 which show that an Hermite factor 1.0109^n can in practice be achieved by BKZ-28 for random lattices while the best proven upper bound for an achievable Hermite factor by BKZ-28 is 1.0282^n.

The original paper was published in

Proceedings STACS 2003,
(Berlin, Germany, February/March 2003)
Eds. H. Alt, M. Habib, Springer-Verlag, LNCS 2607, pages 145–156