Block Reduction for Arbitrary Norms

Michael Kaib* and Harald Ritter†
Fachbereiche Mathematik / Informatik, Universität Frankfurt
60054 Frankfurt am Main, Germany

Abstract

We generalize the concept of block reduction for lattice bases from the l_2–norm to arbitrary norms. This extends the results of Schnorr [S87, S94]. We give algorithms for block reduction and apply the resulting enumeration concept to solve subset sum problems. The deterministic algorithm solves *all* subset sum problems. For up to 66 weights it needs in average less than two hours on a HP 715/50 under HU-UX 9.05.

1 Introduction

Several NP–complete problems can efficiently be reduced to the problem of finding shortest lattice vectors with respect to the l_∞–norm (subset sum, 3–SAT, ...) or the l_1–norm (integer factorization). The known lattice basis reduction concepts and algorithms are based on the Euclidean norm. The first concepts of Lagrange, Gauß and Dirichlet (1773-1850) were developed for low dimensions. The concept of Hermite, Korkine and Zolotarev (1850/73) is strong and algorithmically motivated, but still impractical for higher dimensions. A successful efficient but weak concept was introduced by Lenstra, Lenstra and Lovász [LLL82]. Schnorr [S87] linked Lovász and Hermite's definitions to obtain a flexible hierarchy of concepts, named *block reduction*. Recently some reduction concepts were generalized to arbitrary norms, namely the Lovász–Hermitean by Lovász and Scarf [LS92] and the Gaussian by Kaib and Schnorr [KS94]. In this paper we generalize the strong and efficient concept of block reduction to arbitrary norms. We prove bounds for the quality of block reduced bases and give algorithms to construct them efficiently.

We show that a β-block reduced lattice basis $b_1, \ldots, b_m$ satisfies the inequalites $\frac{4}{i+3}\,\kappa_\beta^{-2\frac{i-1}{\beta-1}} \;\leq\; \| b_i \| / \lambda_i \;\leq\; \frac{i+1}{4}\,\kappa_\beta^{2\frac{m-1}{\beta-1}}$ for arbitrary norms, where the λ_i denote the successive minima and κ_β^2 is a generalization of the Hermite constant γ_β.

*e-mail: kaib@informatik.uni-frankfurt.de
†e-mail: ritter@informatik.uni-frankfurt.de

As practical result we can solve *all* subset sum problems. Up to dimension 66 the deterministic algorithm needs average time less than two hours on a 13.2 MFLOPS workstation. The previous algorithms like the Schnorr–Euchner–algorithm [SE91] only solve a substantial fraction of random subset sum problems.

2 Block Reduced Bases

Given a lattice basis $b_1, \ldots, b_m \in \mathbb{R}^n$ and an arbitrary norm $\|.\|$ we define the distance functions $F_i(x) = min_{\xi_1,\ldots,\xi_{i-1}\in\mathbb{R}} \|x + \sum_{j=1}^{i-1} \xi_j b_j\|$ for all $x \in \mathbb{R}^n$ and $i = 1, \ldots, m$.

Theorem 1. *Every basis $b_1, \ldots, b_m \in \mathbb{R}^n$ of a lattice L satisfies*

$$\min_{i=1,\ldots,m} F_i(b_i) \;\leq\; \lambda_1(L) \;\leq\; \left(m! \prod_{i=1}^{m} F_i\,(b_i) \right)^{1/m} .$$

Proof. The proof of the left–hand inequality follows the proof for the case of the Euclidean norm. For the right–hand inequality let $V_m = \mathrm{vol}_m \{ x \in \mathrm{span}\, L \mid \| x \| \leq 1 \}$ denote the m-dimensional volume of a ball with radius 1. By Minkowski's first Theorem we have the inequality $\lambda_1^m V_m \;\leq\; 2^m \det L$. The Theorem now follows from the inequalities

$$\frac{2^m}{m!\; V_m} \;\leq\; \frac{\prod_{i=1}^m F_i\,(b_i)}{\det L} \;\leq\; \frac{2^m}{V_m} ,$$

which hold for any basis (see [K94], Lemma 5). □

We define the constant κ_m to denote the supremum of $\lambda_1(\mathbb{Z}b_1 + \cdots + \mathbb{Z}b_m) \,/\, \left(\prod_{i=1}^{m} F_i\,(b_i) \right)^{1/m}$ over all lattice bases $b_1, \ldots, b_m$ and all norms on $\mathrm{span}(b_1, \ldots, b_m)$. Here $\lambda_1(L)$ denotes the first successive minimum of the lattice L. For the Euclidean norm we have $\prod_{i=1}^m F_i\,(b_i) = \det L$. The Hermite constants γ_m are defined as the supremum of $\lambda_1^2(L) \det(L)^{-2/m}$ over all lattices L of dimension m. Hence the inequality $\lambda_1(L) \;\leq\; \sqrt{\gamma_m} \left(\prod_{i=1}^{m} F_i\,(b_i) \right)^{1/m}$ holds for the l_2-norm. For the l_2-norm this inequality is sharper than the upper bound of Theorem 1. Theorem 1 shows that

$$\sqrt{\frac{m}{2\pi e}}\,(1 + o(1)) \;\leq\; \sqrt{\gamma}_m \;\leq\; \kappa_m \;\leq\; m!^{1/m} \;= \frac{m}{e}\,(1 + o(1)) .$$

Definition 2. *A lattice basis $b_1, \ldots, b_m \in \mathbb{R}^n$ is called* Hermite reduced*, if*

$$F_i(b_i) \;=\; \min\{F_i(b) \mid b \in \mathbb{Z}b_i + \ldots + \mathbb{Z}b_m - 0\} \text{ for } i = 1, \ldots, m \;.$$

Definition 3. *A lattice basis* $b_1, \ldots, b_m \in \mathbb{R}^n$ *is called* β–block reduced with δ, $\frac{1}{2} \leq \delta \leq 1$, *if for* $i = 1, \ldots, m$

- $\delta F_i(b_i) \;\leq\; \min\{F_i(b) \mid b \in \mathbb{Z}b_i + \ldots + \mathbb{Z}b_{\min(i+\beta-1,m)} - 0\}$ *and*
- $F_j(b_i) \;\leq\; F_j(b_i \pm b_j)$ *for all* $j < i$ *.*

It is called β–block reduced *if it is* β*–block reduced with* $\delta = 1$*.*

For $\beta = 1$ the first condition is empty. A basis $b_1, \ldots, b_m \in \mathbb{R}^n$ is called *size reduced* whenever the second condition is true. It is β–block reduced iff it is size reduced and all blocks $b_i, \ldots, b_{i+j}$ of $j+1$ successive vectors are Hermite reduced with respect to the norm F_i for $j < \beta$, $i + j \;\leq\; m$. For $\beta = m$ every β–block reduced basis is Hermite reduced. For $\beta = 2$ we call them *Lovász reduced with* δ (such bases were introduced for the Euclidean norm by Lenstra, Lenstra and Lovász [LLL82] and studied for arbitrary norms by Lovász and Scarf [LS92]).

For the Euclidean norm, we know from Schnorr [S87, S94] that β–block reduced bases $b_1, \ldots, b_m \in \mathbb{R}^n$ of a lattice L satisfy the inequalities

$$\| b_1 \|_2 \;\leq\; \alpha_{\beta,2}^{\frac{m-1}{\beta-1}} \lambda_1(L) \tag{1}$$

for $\beta - 1 \,|\, m - 1$ and

$$\frac{2}{\sqrt{i+3}}\, \gamma_\beta^{-\frac{i-1}{\beta-1}} \;\leq\; \| b_i \|_2 \,/\, \lambda_i \;\leq\; \frac{\sqrt{i+3}}{2}\, \gamma_\beta^{\frac{m-1}{\beta-1}} \tag{2}$$

Here $\alpha_{k,2}$ is defined to be the supremum of $\| b_1 \|/F_k(b_k)$ over all Hermite reduced lattice bases $b_1, \ldots, b_k$ with respect to the l_2–norm and α_k is the supremum of the same expression over all Hermite reduced lattice bases $b_1, \ldots, b_k$ and all norms. We always have $\alpha_k \leq \alpha_{k+1}$ since the basis $b_0, \ldots, b_k \in \mathbb{R}^{k+1}$ with $b_0 = \lambda_1 e_{k+1}$ is Hermite reduced with respect to the norm $\| \sum_{i=0}^{m} x_i b_i \|_\sim := \max(\| \sum_{i=1}^{m} x_i b_i \|, \; |x_0| \, \lambda_1)$ whenever the basis $b_1, \ldots, b_k \in \text{span}\{e_1, \ldots, e_k\}$ is Hermite reduced with respect to the norm $\| \cdot \|$.

We first generalize Inequality 1 for arbitrary norms:

Theorem 4. *Every* β*–block reduced basis* $b_1, \ldots, b_m \in \mathbb{R}^n$ *of a lattice* L *satisfies*

$$\| b_1 \| \;\leq\; \alpha_\beta^{\lceil \frac{m-1}{\beta-1} \rceil} \lambda_1(L) \;.$$

Proof. Let $h_i := F_i(b_i)$ for $i = 1, \ldots, m$ and choose $\mu \in \{1, \ldots, m\}$ such that $h_\mu = \min h_i$. From $\min_{i=1,\ldots,m} F_i(b_i) \leq \lambda_i$ we get $h_\mu \leq \lambda_1$. The bases $b_i, \ldots, b_{i+j}$ are Hermite reduced with respect to the norm F_i for $0 \leq j < \beta,\ i + j \leq m$. Since the α_k are monotonically increasing we have the inequalities

$$h_i \ \leq \ \alpha_\beta \, h_{i+j}$$

for $0 \leq j < \beta,\ i + j \leq m$. This implies

$$h_1 \ \leq \ \alpha_\beta \, h_{1+(\beta-1)} \ \leq \ \ldots \ \leq \ \alpha_\beta^{\lfloor \frac{\mu-1}{\beta-1} \rfloor} \, h_{1+\lfloor \frac{\mu-1}{\beta-1} \rfloor (\beta-1)} \ \leq \ \alpha_\beta^{\lceil \frac{\mu-1}{\beta-1} \rceil} \, h_\mu \ . \qquad \square$$

For the constants α_β it is known that $\alpha_2 = 2$ [K94]. For $\beta \geq 2$ Schnorr [S87, S94p] proved

$$\alpha_{\beta,2} \leq \ \beta^{\frac{1+\log \beta}{2}} \ , \qquad \alpha_\beta \ \leq \ \beta(\beta-1)^{\log(\beta-1)} \ . \tag{3}$$

Inequality 2 is much stronger than the combination of the bound for $\alpha_{k,2}$ with Inequality 1. This also holds for our generalization of Inequality 2 for arbitrary norms:

Theorem 5. *Every β–block reduced basis $b_1, \ldots, b_m \in \mathbb{R}^n$ of a lattice L satisfies*

$$\left. \begin{array}{l} 2 \leq i \leq m : \ \frac{4}{i+1} \ \kappa_\beta^{-2 \, \frac{i-1}{\beta-1}} \\ 1 \leq i \leq \beta \ : \quad \frac{2}{i+1} \end{array} \right\} \ \leq \ \frac{\| \, b_i \, \|}{\lambda_i} \ \leq \ \left\{ \begin{array}{ll} \frac{i+1}{4} \ \kappa_\beta^{2 \, \frac{m-1}{\beta-1}} : & 1 \leq i \leq m \\ \frac{i+1}{2} & : m-\beta+1 \leq i \leq m \end{array} \right. .$$

Proof. We first prove two lemmata to get the right inequality for $i = 1$:

Lemma 6. *Every β–block reduced basis $b_1, \ldots, b_m \in \mathbb{R}^n$ of a lattice L satisfies*

$$\| \, b_1 \, \| \ \leq \ \left(\prod_{i=1}^{\beta-1} \ \kappa_i^i \right)^{\frac{2}{\beta(\beta-1)}} \ \kappa_\beta^{2 \, \frac{m-\beta}{\beta-1}} \ \max_{i=m-\beta+1}^{m-1} F_i(b_i) \, .$$

Proof. Let $h_i = F_i(b_i)$. By definition the following inequalities hold:

$$h_1^i \ \leq \ \kappa_i^i \ h_1 \cdots h_i \, , \quad \text{for } i = 1, ..., \beta - 1 \ \text{ and}$$

$$h_i^\beta \ \leq \ \kappa_\beta^\beta \ h_i \cdots h_{i+\beta-1} \, , \quad \text{for } i = 1, ..., m - \beta \, .$$

Multiplication of these inequalities yields

$$h_1^{\binom{\beta+1}{2}} h_2^{\beta} \cdots h_{m-\beta}^{\beta} \;\le\; \kappa_1^1\,\kappa_2^2\,\cdots\,\kappa_{\beta-1}^{\beta-1}\,\kappa_\beta^{\beta(m-\beta)}\; h_1^{\beta} h_2^{\beta} \cdots h_{m-\beta}^{\beta} h_{m-\beta+1}^{\beta-1} \cdots h_{m-1}^{1}\,,$$

and this implies

$$\begin{aligned} h_1^{\binom{\beta}{2}} &\le \kappa_1^1\,\kappa_2^2\,\cdots\,\kappa_{\beta-1}^{\beta-1}\,\kappa_\beta^{\beta(m-\beta)} \quad h_{m-\beta+1}^{\beta-1} \cdots h_{m-1}^{1} \\ &\le \kappa_1^1\,\kappa_2^2\,\cdots\,\kappa_{\beta-1}^{\beta-1}\,\kappa_\beta^{\beta(m-\beta)} \left(\max_{i=m-\beta+1}^{m-1} F_i(b_i) \right)^{\binom{\beta}{2}} . \end{aligned}$$

□

Lemma 7. *Every β–block reduced basis $b_1, \ldots, b_m \in \mathbb{R}^n$ of a lattice L satisfies*

$$\| b_1 \| \;\le\; \left(\prod_{i=1}^{\beta-1} \kappa_i^i \right)^{\frac{2}{\beta(\beta-1)}} \kappa_\beta^{2\,\frac{m-\beta}{\beta-1}}\; \lambda_1(L)\;.$$

Proof. The lemma follows from Lemma 6 by induction over m. For $m = \beta$ the lemma holds by definition 3. Let now $b = r_1 b_1 + \ldots + r_m b_m$ be a shortest lattice vector. For $r_m = 0$ the claim holds by assumption. For $r_m \neq 0$ we have the inequalities

$$\lambda_1(L) \;=\; \| b \| \;\ge\; F_i(b) \;\ge\; F_i(b_i) \text{ for } m-\beta+1 \le i \le m\,,$$

and the lemma follows with Lemma 6. □

Iteration of the inequality $\kappa_{m+1}^{m+1} \ge 2\kappa_m^m$ [K94] yields the first inequality of the theorem by Lemma 7:

$$\| b_1 \| \;\le\; \frac{1}{2}\; \kappa_\beta^{2\,\frac{m-1}{\beta-1}}\; \lambda_1(L)\,. \tag{4}$$

Proof of the right inequality of Theorem 5. For every $j \le m$ the basis $b_j, \ldots, b_m$ is β–block reduced with respect to the norm F_j. Hence $F_j(b_j) = \lambda_{1,F_j}(\mathbb{Z} b_j + \ldots + \mathbb{Z} b_m)$ for $m - \beta + 1 \le j \le m$ and, by Inequality 4:

$$F_j(b_j) \;\le\; \tfrac{1}{2}\; \kappa_\beta^{2\,\frac{m-1}{\beta-1}}\; \lambda_{1,F_j}(\mathbb{Z} b_j + \ldots + \mathbb{Z} b_m)\,.$$

for $1 \le i \le m$. In addition, we have $\lambda_{1,F_j}(\mathbb{Z}b_j + \ldots + \mathbb{Z}b_m) \le \lambda_j(L) \le \lambda_i(L)$ for $j \le i$. The upper bound is now a consequence of the inequality

$$\| b_i \| \ \le \ F_i(b_i) \ + \ \frac{1}{2} \sum_{j=1}^{i-1} F_j(b_j) \ . \tag{5}$$

We show the correctness of Inequality 5 for any size reduced basis: Let $F_j(b_i + \xi_0 b_j) = \min_{\xi \in \mathbb{R}} F_j(b_i + \xi b_j) = F_{j+1}(b_i)$. The fact that $F_j(b_i) \ \le \ F_j(b_i \pm b_j)$ for $j < i$ implies

$$\begin{aligned} F_j(b_i) \ &= \ \min_{\mu \in \mathbb{Z}} F_j(b_i + \mu b_j) \\ &\le \ F_j(b_i + \lfloor \xi_0 \rceil b_j) \\ &= \ F_j \left(b_i + \xi_0 b_j \ + \ (\lfloor \xi_0 \rceil - \xi_0) \ b_j \right) \\ &\le \ F_{j+1}(b_i) + \frac{1}{2} F_j(b_j) \ , \end{aligned}$$

since F_j is a norm. Successive application of this inequality for $j = 1, \ldots, i-1$ shows inequality 5.

Proof of the left inequality of Theorem 5. By definition of the successive minima and because of Inequality 5 we have

$$\lambda_i \ \le \ \max_{j=1}^{i} \| b_j \| \ \le \ \frac{i+1}{2} \max_{j=1}^{i} F_j(b_j) \ .$$

Theorem 5 is now a consequence of the inequalities $F_j(b_j) \le \| b_i \|$ for $i - \beta + 1 \le j \le i$ and

$$F_j(b_j) \ \le \ \tfrac{1}{2} \ \kappa_\beta^{2 \frac{i-j}{\beta - 1}} \ \| b_i \| \qquad \text{for } 1 \le j < i \ . \tag{6}$$

The Inequalities 6 are obvious: every basis $b_j, \ldots, b_i$ is β–block reduced with respect to the norm F_j. Hence Lemma 6 bounds the first heights for $1 \le j \le i - \beta + 1$ by the last ones:

$$F_j(b_j) \ \le \ \tfrac{1}{2} \ \kappa_\beta^{2 \frac{i-j}{\beta - 1}} \ \max_{h=i-\beta+1}^{i-1} F_h(b_h) \ .$$

By definition 3 the last heights for $i - \beta + 1 \le j \le i$ we get the inequalities

$$F_j(b_j) \ \le \ F_j(b_i) \ \le \ \| b_i \| \ . \qquad \square$$

3 Algorithms for β–Block Reduction

Algorithm β–Block Reduce
INPUT: $b_1, \ldots, b_m \in \mathbb{Z}^n$, δ with $1/2 \leq \delta \leq 1$, β with $2 \leq \beta \leq m$
1. size reduce $b_1, \ldots, b_m$, $j := m-1, z := 0$
2. WHILE $z < m-1$
$j := j+1$, IF $j = m$ THEN $j = 1$
$k := \min(j+\beta-1, m)$
ENUM(j,k) (this finds the minimal place $(u_j, \ldots, u_k) \in \mathbb{Z}^{k-j+1} - 0^{k-j+1}$
and the minimal value $\bar{F}_j = F_j(\sum_{i=j}^{k} u_i b_i)$
and also $b_j^{\text{new}} := \sum_{i=j}^{k} u_i b_i$)
$h := \min(k+1, m)$
IF $\bar{F}_j < \delta F_j(b_j)$
THEN extend $b_1, \ldots, b_{j-1}, b_j^{\text{new}}$
to a basis $b_1, \ldots, b_{j-1}, b_j^{\text{new}}, \ldots, b_h^{\text{new}}$ of $L(b_1, \ldots, b_h)$
size reduce $b_1, \ldots, b_{j-1}, b_j^{\text{new}}, \ldots, b_h^{\text{new}}$, $z := 0$
ELSE size reduce $b_1, \ldots, b_h$
$z := z+1$
END while
OUTPUT: $b_1, \ldots, b_m$

COMMENTS. 1. Throughout the algorithm the integer j is cyclically shifted through the integers $1, 2, \ldots, m-1$. The variable z counts the number of positions j that satisfy the inequality $\delta F_j(b_j) \leq \bar{F}_j$. If this inequality does not hold for j then we insert b_j^{new} into the basis, we size reduce and we reset z to 0. The integer $j = m$ is skipped since the inequality always holds for $j = m$. Obviously a basis $b_1, \ldots, b_m$ is β–block reduced with δ if it is size reduced and $z = m-1$. Therefore the algorithm produces, up to floating point errors, a basis that is β–block reduced with δ.
2. We can extend $b_1, \ldots, b_{j-1}, b_j^{new}$ to a basis $b_1, \ldots, b_{j-1}, b_j^{new}, \ldots, b_h^{new}$ of the lattice $L(b_1, \ldots, b_h)$ using the coefficients u_i in the representation $b_j^{new} = \sum_{i=j}^{h} u_i b_i$. For this we compute $T \in GL_{h-j+1}(\mathbb{Z})$ with $[u_j, \ldots, u_h]T = [1, 0, \ldots, 0]$ and we set $[b_j^{new}, \ldots, b_h^{new}] := [b_j, \ldots, b_h]T^{-1}$.

ENUM(j,k)
1. $(u_j, \ldots, u_k) := (1, 0, \ldots, 0), (\tilde{u}_j, \ldots, \tilde{u}_k) := (1, 0, \ldots, 0), s := t := j, b_j^{new} := b_j, \bar{F}_j := F_j(b_j)$
2. WHILE $t \leq k$
IF $F_t(\sum_{i=t}^{s} \tilde{u}_i b_i) < \bar{F}_j$
THEN IF $t > j$
THEN $t := t-1$

find $z \in \mathbb{R}$ with $F_t(zb_t + \sum_{i=t+1}^{s} \tilde{u}_i b_i) = F_{t+1}(\sum_{i=t+1}^{s} \tilde{u}_i b_i)$
$l_t := \lfloor z \rfloor, r_t := l_t + 1$
IF $F_t(l_t b_t + \sum_{i=t+1}^{s} \tilde{u}_i b_i) < F_t(r_t b_t + \sum_{i=t+1}^{s} \tilde{u}_i b_i)$
THEN $\tilde{u}_t := l_t, l_t := l_t - 1$
ELSE $\tilde{u}_t := r_t, r_t := r_t + 1$
ELSE $(u_j, \ldots, u_k) := (\tilde{u}_j, \ldots, \tilde{u}_k), b_j^{new} := \sum_{i=j}^{s} \tilde{u}_i b_i, \bar{F}_j := F_j(b_j^{new})$
ELSE $t := t + 1$
IF $t \geq s$
THEN $\tilde{u}_t := \tilde{u}_t + 1$
$s := t$
ELSE
IF $F_t(l_t b_t + \sum_{i=t+1}^{s} \tilde{u}_i b_i) < F_t(r_t b_t + \sum_{i=t+1}^{s} \tilde{u}_i b_i)$
THEN $\tilde{u}_t := l_t, l_t := l_t - 1$
ELSE $\tilde{u}_t := r_t, r_t := r_t + 1$
END while
Output: $(u_j, \ldots, u_k), \bar{F}_j, b_j^{new}$

The minimum of F_j is searched in the sublattices $L(b_j, \ldots, b_s)$ with increasing s. In every stage of the algorithm we have $\tilde{u}_s > 0$, i.e. the vector b_s is used positively for the search. This prevents redundancies during the enumeration. At every step t of algorithm ENUM(j,k) we have already fixed the integers $\tilde{u}_{t+1}, \ldots, \tilde{u}_s$. We enumerate the integers $\tilde{u}_t$ in order of ascending values $F_t(\sum_{i=t}^{s} \tilde{u}_i b_i)$. For this purpose we calculate a real number z for which $F_t(zb_t + \sum_{i=t+1}^{s} \tilde{u}_i b_i)$ is minimal. An integral minimal place $\tilde{u}_t$ is one of the integers $l_t = \lfloor z \rfloor$ or $r_t = \lceil z \rceil$ because of convexity. If $F_t(l_t b_t \sum_{i=t+1}^{s} \tilde{u}_i b_i) \geq F_j(\sum_{i=j}^{k} u_i b_i)$, then this inequality holds for all $\tilde{u}_t < l_t$, i.e. we can stop the enumeration to the left. Similiarly we can stop the enumeration to the right whenever $F_t(r_t b_t + \sum_{i=t+1}^{s} \tilde{u}_i b_i) \geq F_j(\sum_{i=j}^{k} u_i b_i)$. When enumeration of l_t (r_t) is finished we look at $l_t - 1$ ($r_t + 1$) instead. The complexity of computing F_t and the corresponding coefficient z as well as the number of computations of F_t is crucial for the complexity of the whole algorithm.

4 Enumeration with Respect to l_p–Norms

With respect to the Euclidean norm we can efficiently calculate $z \in \mathbb{R}$ and F_t. For this we define $\mu_{i,j} := \frac{<b_i, \hat{b}_j>}{<\hat{b}_j, \hat{b}_j>}$, $\pi_i(b_j) := b_j - \sum_{t=1}^{i-1} \mu_{i,t} \hat{b}_t$, $\hat{b}_j := \pi_j(b_j)$, $c_i :=< \hat{b}_i, \hat{b}_i >= \|\hat{b}_i\|_2^2$ and $\tilde{c}_t := \|\pi_t(\sum_{i=t}^{k} \tilde{u}_i b_i)\|_2^2$ for $1 \leq i, j \leq m$. We obtain $z = -\sum_{i=t+1}^{k} \tilde{u}_i \mu_{i,t}$, $F_t^2(\sum_{i=t}^{k} \tilde{u}_i b_i) = \tilde{c}_t = \tilde{c}_{t+1} + (\tilde{u}_t + z)^2 c_t$.

For general l_p–norms we use the fact that all norms on $\mathbb{R}^n$ are equivalent. There exist constants $r_p, R_p > 0$ such that for all $x \in \mathbb{R}^n \quad r_p\|x\|_p \leq \|x\|_2 \leq R_p\|x\|_p$.
With $w_t = w_t(\tilde{u}_t, \ldots, \tilde{u}_k) := \pi_t(\sum_{i=t}^k \tilde{u}_i b_i)$, $Q_{p,1} := 1$ and $Q_{p,j} := R_p/r_p$ for $j > 1$ we get $w_t = w_{t+1} + (\tilde{u}_t + y_t)\hat{b}_t$ and $\|\pi_j(x)\|_p \leq Q_{p,j}F_j(\pi_j(x))$.

Lemma 8. *If, for fixed $(\tilde{u}_t, \ldots, \tilde{u}_k) \in \mathbb{Z}^{k-t+1}$, there is some $(\tilde{u}_j, \ldots, \tilde{u}_{t-1}) \in \mathbb{Z}^{t-1}$ with $F_j(\sum_{i=j}^k \tilde{u}_i b_i) < F_j(b_j)$, then the following inequality holds for all $\lambda_t, \ldots, \lambda_m \in \mathbb{R}$:*

$$|\sum_{i=t}^m \lambda_i \tilde{c}_i| < Q_{p,j}F_j(b_j)\|\sum_{i=t}^m \lambda_i w_i\|_q \tag{7}$$

Proof. For fixed $(\tilde{u}_l, \ldots, \tilde{u}_k)$ we enumerate vectors w_i on stages $1, \ldots, l-1$ which are all in the hyperplane orthogonal to w_l. We have $w_i - w_l - w_l$ for $i < l$, i.e.

$$< w_i, w_l > - < w_l, w_l > = < w_i - w_l, w_l > = 0. \tag{8}$$

If we can complete $(\tilde{u}_t, \ldots, \tilde{u}_k)$ to $(\tilde{u}_j, \ldots, \tilde{u}_k)$ with $0 < F_j(w_j) = F_j(\sum_{i=j}^k \tilde{u}_i b_i) < F_j(b_j)$, then $\|w_i\|_2^2 < Q_{p,j}F_j(w_j)\|w_i\|_q$ for $i = t, \ldots, m$ because of $| < w_j, w_l > | \leq \|w_j\|_p\|w_l\|_q$ (Hölder's inequality, $1/p + 1/q = 1$) and $\|w_j\|_p \leq Q_{p,j}F_j(w_j)$. We obtain

$$\begin{aligned} |\sum_{i=t}^k \lambda_i \tilde{c}_i| &= |\sum_{i=t}^k \lambda_i < w_i, w_i > | = |\sum_{i=t}^k \lambda_i < w_i, w_j > | = | < \sum_{i=t}^k \lambda_i w_i, w_j > | \\ &\leq \|w_j\|_p\|\sum_{i=t}^k \lambda_i w_i\|_q < Q_{p,j}F_j(b_j)\|\sum_{i=t}^m \lambda_i w_i\|_q. \end{aligned}$$

□

The main goal is an optimal selection of vectors $(\lambda_t, \ldots, \lambda_k)$ for which we test Inequality 7.

Some special vectors:

- $(\lambda_t, \ldots, \lambda_k) = (1, 0, \ldots, 0)$: Compare $\tilde{c}_t$ and $Q_{p,j}F_j(b_j)\|w_t\|_q$. This linear test will result in a search tree which is (for $p = 1$ and $p = \infty$) exponentially smaller than the full enumeration tree (no pruning) without any additional test.
- $(\lambda_t, \ldots, \lambda_k) = (\lambda, 1-\lambda, 0, \ldots, 0)$ with $\lambda \in]0, 1[$: For the whole line $\lambda w_t + (1-\lambda)w_{t+1}$ we need $\lambda\tilde{c}_t + (1-\lambda)\tilde{c}_{t+1} < Q_{p,j}F_j(b_j)\|\lambda w_t + (1-\lambda)w_{t+1}\|_q$, especially for all points w_t' between w_{t+1} and w_t. These points were enumerated before w_t.
  Because of $\|\lambda w_t + (1-\lambda)w_{t+1}\|_2^2 \leq \lambda\tilde{c}_t + (1-\lambda)\tilde{c}_{t+1}$ we can stop the enumeration in direction $w_t - w_{t+1}$ as soon as the test with $(1, 0, \ldots, 0)$ causes a break.

Algorithm ENUM$_p$

INPUT $j, k, n, p, q, R_p, Q_{p,j}$, c_i, b_i, $\hat{b}_i$ for $i = j, \ldots, k$ and $\mu_{i,t}$ for $j \le t < i \le k$

1. $s := t := j$, $\tilde{u}_j := u_j := 1$, $y_j := \Delta_j := 0$, $\eta_j := \delta_j := 1$, $w_j := (0, \ldots, 0)$
   FOR $i = j+1, \ldots, k+1$
   $\tilde{c}_i := u_i := \tilde{u}_i := y_i := \Delta_i := 0, \eta_i := \delta_i := 1$, $w_i := (0, \ldots, 0)$
   $\bar{F} := F_j(b_j)$, $\hat{F} := R_p^2 \bar{F}^2$
2. WHILE $t \le k$
   $\tilde{c}_t := \tilde{c}_{t+1} + (y_t + \tilde{u}_t)^2 c_t$
   IF $\tilde{c}_t < \hat{F}$
   THEN $w_t := w_{t+1} + (y_t + \tilde{u}_t)\hat{b}_t$
   IF $t > j$
   THEN IF PRUNE$(t, s, n, \bar{F}, w_t, \ldots, w_s, \tilde{c}_t, \ldots, \tilde{c}_s, q, Q_{p,j})$=1
   THEN IF $\eta_t = 1$ THEN GOTO 3.
   $\eta_t := 1$, $\Delta_t := -\Delta_t$
   IF $\Delta_t \delta_t \ge 0$ THEN $\Delta_t := \Delta_t + \delta_t$
   $\tilde{u}_t := v_t + \Delta_t$
   ELSE $t := t - 1$, $\eta_t := \Delta_t := 0$, $y_t := \sum_{i=t+1}^{s} \tilde{u}_i \mu_{i,t}$
   $\tilde{u}_t := v_t := \lceil -y_t \rfloor$
   IF $\tilde{u}_t > -y_t$ THEN $\delta_t := -1$
   ELSE $\delta_t := 1$
   ELSE IF $F_j(w_j) < \bar{F}$
   THEN $u_i := \tilde{u}_i$ for $i = j, \ldots, s$
   $\bar{F} := F_j(w_j), \hat{F} := R_p^2 \bar{F}^2$
3. ELSE $t := t + 1$
   $s := \max(t, s)$
   IF $\eta_t = 0$
   THEN $\Delta_t := -\Delta_t$
   IF $\Delta_t \delta_t \ge 0$ THEN $\Delta_t := \Delta_t + \delta_t$
   ELSE $\Delta_t := \Delta_t + \delta_t$
   $\tilde{u}_t := v_t + \Delta_t$

   END while

OUTPUT $(u_j, \ldots, u_k), \bar{F}, b_j^{new} = \sum_{i=j}^{k} u_i b_i$

Algorithm PRUNE$(\mathbf{t}, \mathbf{s}, \mathbf{n}, \bar{\mathbf{F}}, \mathbf{w_t}, \ldots, \mathbf{w_s}, \tilde{\mathbf{c}}_\mathbf{t}, \ldots, \tilde{\mathbf{c}}_\mathbf{s}, q, Q_{p,j})$:

Test for several $(\lambda_t, \ldots, \lambda_s)$ with $\lambda_t \ne 0$ and $\sum_{i=t}^{s} \lambda_i \tilde{c}_i > 0$, whether $\sum_{i=t}^{s} \lambda_i \tilde{c}_i < Q_{p,j} \bar{F} \| \sum_{i=t}^{s} \lambda_i w_i \|_q$. If the inequality doesn't hold for any $(\lambda_t, \ldots, \lambda_s)$ then return 1, else return 0.

Remark 9. η_t indicates the number of directions in which the enumeration is already stopped at stage t. Whenever $\eta_t = 1$ and PRUNE$(t, \ldots) = 1$ we can increase t by 1. We avoid redundancies by choosing $\tilde{u}_s > 0$ and initialize $\eta_s = 1$. We shrink the choice

of $(\lambda_t, \ldots, \lambda_s)$ to the case $\lambda_t \neq 0, \quad \sum_{i=t}^{s} \lambda_i \tilde{c}_i > 0$ to simplify the algorithm. If we allow arbitrary $(\lambda_t, \ldots, \lambda_s)$ we have to decide in which direction we can stop the enumeration.

In the case of $p = 2$ PRUNE$(t, \ldots)$ is always 0. Hence we can simplify the algorithm. We don't need the vectors w_t and η.

5 Solving Subset Sum Problems

Given positive integers $a_1, \ldots, a_n, s$ we wish to solve the equation $\sum_{i=1}^{n} x_i a_i = s$ with $x_1, \ldots, x_n \in \{0, 1\}$. As in [SE91] we assume the existence of a solution and the knowledge of $g := \sum_{i=1}^{n} x_i$. We consider the following lattice basis:

$$B = (b_1, \ldots, b_{n+1})^T = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 & 2s & 2g \\ 0 & 2 & 0 & \cdots & 0 & 2a_1 & 2 \\ 0 & 0 & 2 & & 0 & 2a_2 & 2 \\ \vdots & & \ddots & \ddots & \vdots & \vdots & \vdots \\ 0 & \cdots & & & 2 & 2a_n & 2 \end{pmatrix}$$

Without knowledge of g we have to remove the last column of the basis. In this case the running time is moderately higher (in average we lose a factor 2). Every lattice vector $b = \sum_{i=1}^{n+1} t_i b_i$ with $\|b\|_\infty = 1$ yields a solution of the subset sum problem. The following deterministic lattice basis reduction algorithm is designed to solve *every* subset sum problem:

1. L^3–reduce B with $\delta = 0.99$ and 5 deep insertions. Test for a solution after every reduction step. For details, see [SE91].

2. Transform the basis to get only two vectors with nonzero entries in the last two columns. Delete these vectors and the last two columns (the deleted vectors cannot yield any solution).

3. β–block reduce B with $\delta = 0.99$ and 5 deep insertions. Test for a solution after every reduction step. For details, see [SE91].

4. Call algorithm ENUM$_p$ with $j = 1, \ k = n - 1, \ p = \infty, \ q = 1$; initialize $\bar{F}$ with $1 + \epsilon$ and stop the enumeration as soon as a vector with l_∞–norm 1 was found. (We have $R_\infty = \sqrt{n}, \ r_\infty = 1$ and $Q_{\infty,1} = 1$.)

Steps 1 and 3 are done with respect to the Euclidean norm. For general subset sum problems up to dimension 66 we can restrict the test PRUNE(t,...) to $(\lambda_t, \ldots, \lambda_k) = (1, 0, \ldots, 0)$.

Practical Results. We compare the new results with the results of Schnorr–Euchner [SE91]. For every dimension n and every bitlength b (of the weights a_i) we generated 20 random problems with $g = n/2$ as follows: Pick random numbers $a_1, \ldots, a_n$ in the interval $[1, 2^b]$, pick a random subset $I \subset \{1, \ldots n\}$ of size g, set $s = \sum_{i \in I} a_i$. The probabilistic algorithm of Schnorr–Euchner permutes the basis before β–block reducing it (partially pruned) with respect to the Euclidean norm. This will be done at most 16 times. The running times give the average CPU-time per problem on a HP Apollo 715/50 (13.2 MFLOPS). The times of the Schnorr–Euchner statistic are converted to this computer type.

		Schnorr–Euchner block size 50, pruned				new block zize 30, no pruning			
n	b	succ. round 1	succ. total	rounds	time h:mm:ss	succ. BKZ	succ. Enum	succ. total	time h:mm:ss
66	34	20	20	20	0:01:34	20	0	20	0:00:29
66	42	20	20	20	0:06:22	17	3	20	0:13:39
66	50	10	19	78	0:36:08	11	9	20	1:50:54
66	58	9	14	119	1:28:10	13	7	20	1:11:45
66	66	10	19	70	1:14:17	12	8	20	1:06:17
66	72	18	20	26	0:31:21	17	3	20	0:18:42
66	80	20	20	20	0:15:16	19	1	20	0:04:05
66	88	20	20	20	0:14:28	20	0	20	0:02:20
Σ		127	152	373		129	31	160	

Acknowledgment. We are grateful to Claus Schnorr for stimulating successful teamwork and motivating helpful discussions.

References

[KS94] M. Kaib, C.P. Schnorr: The Generalized Gauss Reduction Algorithm. (1993), 13 pages. To appear in Journal of Algorithms.

[K94] M. Kaib: Gitterbasenreduktion für beliebige Normen. Ph.D. thesis, Universität Frankfurt, 1994.

[LLL82] A.K. Lenstra, H.W. Lenstra, Jr., L. Lovász: Factoring polynomials with rational coefficients. Math. Annalen 261 (1982), pp. 515-534.

[LS92] L. Lovász, H. Scarf: The Generalized Basis Reduction Algorithm. Mathematics of Operations Research, vol. 17, No. 3 (1992), pp. 754-764.

[S87] C.P. Schnorr: A Hierarchy of Polynomial Time Lattice Basis Reduction Algorithms. Theoretical Computer Science 53 (1987), pp. 201-224.

[S94] C.P. Schnorr: Block reduced lattice bases and successive minima. Technical Report, ICSI Berkeley (1992), 18 pages. To appear in Combinatorics, Probability and Computing.

[S94p] C.P. Schnorr: Private correspondence. (1994), 2 pages.

[SE91] C.P. Schnorr, M. Euchner: Lattice basis reduction: improved algorithms and solving subset sum problems. Proceedings of the FCT'91, SLNCS 529 (1991), pp. 68-85. To appear in Mathematical Programming Studies.