Generating Hard Instances of the Short Basis Problem

Miklós Ajtai

IBM Almaden Research Center, CA 95120, USA

Abstract. A class of random lattices is given, in [1] so that (a) a random lattice can be generated in polynomial time together with a short vector in it, and (b) assuming that certain worst-case lattice problems have no polynomial time solutions, there is no polynomial time algorithm which finds a short vector in a random lattice with a polynomially large probability. In this paper we show that lattices of the same random class can be generated not only together with a short vector in them, but also together with a short basis. The existence of a known short basis may make the construction more applicable for cryptographic protocols.

1. Introduction. Most of the well-known, hard computational problems, (e.g. factoring), are worst-case problems, while for cryptographic applications we need hard average-case problems. The reason is that any random instance of a hard average case problem is also hard with a positive probability, while there is no known way that would create a hard instance of a hard worst-case problem. Using lattice problems it is possible to create average-case problems which are just as difficult as certain well-known worst-case problem. For a more detailed description of the worst-case, average-case connection and for cryptographic applications see e.g. [1], [2], [4], [5], [6], [7] or the survey paper [3]. (Further references are given in [3].) One of the worst-case lattice problems used in [1] is the following:

(**P**) *Find a basis $b_1, ..., b_n$ in the n-dimensional lattice L whose length, defined as $\max_{i=1}^{n} \|b_i\|$, is the smallest possible up to a polynomial factor.*

We will refer to this problem as the short basis problem. It is proved in [1] that if (**P**) has no polynomial time solution then a random lattice L can be generated in polynomial time (with a suitably chosen distribution), together with a vector shorter than $\sqrt{n}$ in it, so that, for any algorithm $\mathcal{A}$ the probability that $\mathcal{A}$ finds in L a vector shorter than $\sqrt{n}$, if L is given as an input, is smaller than n^{-c} (for any fixed $c > 0$ if n is sufficiently large). That is, using the assumption that the worst-case short basis problem is hard, we are able to create a hard instance of the short vector problem with a known solution. In this paper we show that instead of the short vector problem we may use the short basis problem in the conclusion of the theorem as well, in the strong sense that we construct the random lattice together with a short basis, but to find even a short vector in it is difficult. This last property will be a consequence of the fact that we are

J. Wiedermann et al. (Eds.): ICALP'99, LNCS 1644, pp. 1–9, 1999.

using the same random class of lattices as in [1], we only modify the way as a random lattice is generated, without changing it's distribution (by more than an exponentially small error). (These type of random lattices where a short basis is known for the person who generates the lattice, but nobody else can find even a short vector, seem to be more suitable for cryptographic applications, than the ones generated together with a single short vector. We intend to return to this question in a separate paper. The public-key crypto-system of Goldreich, Goldwasser and Halevi described in [6] is based on the availability of a short basis. However the size of a basis is defined in a different way, so our random lattice together with the generated basis probably does not meet the requirements of their system.) The dimension of the lattice for the average-case problem is larger than for the corresponding worst-case problem. If the dimension of the lattice in the worst-case problem is n, then the dimension of the lattice in the average case problem is $c'n \log n$ for a suitably chosen constant $c' > 0$. We will use the same construction for a random lattice as was used in [1], (more precisely the distance of the distributions of the random lattices used in the two papers is exponentially small in n). To give an exact formulation of our result we recall the definition of the random lattice form [1] with a somewhat modified notation. (n will denote now the dimension of the random lattice.)

Assume that the positive integers q, r, n, $r < n$ are fixed. (The results of [1] hold if $r^{c_1} < q < 2r^{c_1}$ and $r^{c_3} > n \geq c_2 r \log r$ for some suitably chosen absolute constants c_1, c_2, c_3.) Let I_i^j be the set of all j dimensional vectors whose coordinates are from the set $\{0, 1, ..., i-1\}$. First we pick a random sequence $u_0, ..., u_{n-1}$ independently and with uniform distribution from the set I_q^r. The random lattice L will consist of all sequences of integers $h_0, ..., h_{n-1}$ so that

$$\sum_{i=0}^{n-1} h_i u_i \equiv 0 \pmod{q}$$

The distribution of L will be denoted by Γ_n.

This definition gives an explicit way of generating lattices in the random class. In [1], with a slight modification of this definition, we were able to generate almost the same distribution (with an exponentially small error) together with a short vector in L. Namely, first we randomize only $u_0, ..., u_{n-2}$ independently and with uniform distribution from I_q^r and independently from that a random $0, 1$ sequence $\delta_0, ..., \delta_{n-2}$, with uniform distribution on the set of all $0, 1$ sequences of length $n-1$. Let u_{n-1} be the smallest nonnegative residue modulo q of

$$-\sum_{i=0}^{n-2} \delta_i u_i$$

(where we take the residue of each component of the vector). This way we have defined the sequence $u_0, ..., u_{n-1}$ and from this we can define the lattice the same way as in the original definition. The distribution of this lattice will be denoted by Γ'_n. The sequence $v = \langle \delta_0, ..., \delta_{n-2}, 1 \rangle$ will be in the lattice and its length is at most $\sqrt{n}$. (It is shown in [1] that if (**P**) has no polynomial time solutions, then

such a short vector cannot be found in polynomial time with a polynomially large probability, provided that the sequence $u_0, ..., u_{n-1}$ is given as an input.) We define the distance of two probability dstributions P_1 and P_2 on the same σ-algebra X as $\max\{|P_1(A) - P_2(A)| + |P_1(B) - P_2(B)| \mid A, B \in X, A \cap B = \emptyset\}$

Theorem 1. *There is a $c > 0$ so that for each positive integer n there is a distribution Φ_n on the set of n dimensional lattices so that the distance of the distributions Γ_n and Φ_n is at most 2^{-cn}, moreover a random lattice L according to the distribution Φ_n, can be generated in polynomial time together with a basis in it whose length, (that is, the maximum of the lengths of it's elements) is at most $n^3\sqrt{n}$.* □

Remark. The results of [1] imply that if there is no polynomial time solution for (**P**), then there is no algorithm which finds a vector shorter than $\sqrt{n}$ in a random L (according to the distribution Γ_n) with a probability greater then $n^{-c'}$, for any $c' > 0$ if n is sufficiently large. Since the distance of the distributions Γ_n, Φ_n is exponentially small this holds for the distributions Φ_n as well. That is, as we claimed earlier, we are able to generate a random lattice together with a short basis, so that it is hard to find even a short vector in the random latttice, if only the lattice is given as an input, provided that the worst-case problem (**P**) is hard.

2. The proof of the theorem. In the proof of our theorem we will use the following lemma from [1]. (There the lemma is used in the proof of the fact that the distance of Γ_n and Γ'_n is exponentially small in n.)

Lemma A. *There exists a $c > 0$ so that if A is a finite Abelian group with n elements and k is a positive integer and $b = \langle b_1, ..., b_k \rangle$ is a sequence of length k whose elements are chosen independently and with uniform distribution from A, then with a probability of at least $1 - 2^{-ck}$ the following holds:*

Assume that b is fixed and we randomize a $0,1$-sequence $\delta_1, ...\delta_k$, where the numbers δ_i are chosen independetly and with uniform distribution from $\{0,1\}$. For each $a \in A$ let $p_a = P(a = \sum_{i=1}^{k} \delta_i b_i))$. Then

(a) $\sum_{a \in A}(p_a - |A|^{-1})^2 \leq 2^{-2ck}$ *and*

(b) $\sum_{a \in A} |p_a - |A|^{-1}| \leq |A|^{\frac{1}{2}} 2^{-ck}$.

If $A = I_q^r$ (with the modulo q addition) then this lemma shows that for almost all fixed values of $u_0, ..., u_{n-2}$ if $\delta_0, ..., \delta_{n-2}$ is picked at random then the distribution of

$$\sum_{i=0}^{n-2} \delta_i u_i = -u_{n-1}$$

is almost uniform on I_q^r.

This construction gives a single short vector v in L. We want to modify it so that we get a short basis of L. Short will mean now that the Euclidean norm of each basis vector is at most $n^3\sqrt{n}$.

To make our construction simpler we assume that q is odd. (We will prove the independence of the constructed vectors by showing that their determinant is odd.) Instead of generating a short basis of L we will generate first only n linearly independent vectors and then from them we can get a basis of L while we increase their length only by a factor of n. (See [1])

There is an easy way to generate the random lattice L together with more than one short vector. Namely we randomize only $u_0, ..., u_{n-1-s}$ for some fixed s and define the remaining $u_{n-s}, ..., u_{n-1}$ as their linear combinations with random $0, 1$ coefficients. If $n - s > c \log |A| = c \log(q^r) = c' r \log r$ then Lemma A remains applicable and we get s linearly independent vectors. Although this cannot be improved further, we keep the idea of randomizing certain vectors u_i and get the other ones as their random linear combinations in our final construction. (The coefficients in this construction will not be $0, 1$ and their distribution will not be uniform.) More precisely we will get the random sequence $u_0, ...u_{n-1}$ in the following way:

We randomize first only r vectors $u_0, ..., u_{r-1}$ independently and with uniform distribution from I_q^r. Let Y be an n by r matrix whose first r rows are $u_0, ..., u_{r-1}$ and the remaining entries are variables. Let T be the set of these variables. We will define a random n by n matrix A' (with integer entries) depending on the vectors $u_0, ..., u_{r-1}$. The distribution of the matrix A' is the crucial part of the definition; we will give it later. Assume that A' has been chosen. A will be the matrix consisting of the first $n-r$ rows of A'. Consider that equation $AY = 0$. We will define A' so that this equation has a unique rational solution for the variables in T, moreover this solution assigns integer values for all of these variables. Substituting these values into Y and then taking their least nonnegative residue modulo q we get a matrix Y'. The rows of Y' will be $u_0, ..., u_{n-1}$. We will show that $A'Y' \equiv 0 \pmod q$. The rows of A' will be short linearly independent elements of L. The congruence $A'Y' \equiv 0 \pmod q$ imples that that the rows of A' are indeed elements of L. Using the definition of A' we will show that they are short and linearly independent.

We define A' in two parts. First we define only A, an $n - r$ by n matrix. A will be the first $n - r$ rows of A'. Then separately we define the last r rows of A'. A together with $u_0, ..., u_{r-1}$ will already determine the sequence $u_0, ..., u_{n-1}$.

The first r columns of the matrix A forms an $n - r$ by r matrix this will be denoted by A_1. The remaining columns form a square ($n - r$ by $n - r$) matrix A_2. Let $\mu = [\log_r q] + 2$

We will start the numbering of the rows and columns of each matrix with 0. That is, an i by j matrix D has rows $0, 1, ..., i - 1$ and columns $0, 1, ..., j - 1$. If $D = \{d_{s,t}\}_{s=0,...,i-1,t=0,...j-1}$ then we say that $d_{s,t}$ is the tth elements of the sth row. When we say "the first k rows of the matrix D" we refer to rows $0, 1, ..., k-1$.

Definition of A_1. The ith element of the μith row is 1 for $i = 0, ..., r - 1$, all of the other entries are 0.

Definition of A_2. We will define A_2 as $A_2 = BC$ where B, C are $n-r$ by $n-r$ matrices.

Later we will give a concise but technical definition of the matrices B and C. Now we give a more easily understandable but longer definition, together with the motivating ideas. Let X be an $n-r$ by r matrix, consisting of the last $n-r$ rows of Y, that is containing only the variables, and let U be an $n-r$ by r matrix whose $i\mu$th row is u_i for $i = 0, ..., r$ and all other rows have all 0 entries. The definition of A_1 implies that the equation $AY = 0$ is equivalent to the equation $A_2X = -U$. We we want to define the matrix $A_2 = BC$ in a way that will make it easy to get an explicit description of the solution of the equation $BCX = -U$. B will be a lower triangular matrix with integer entries and 1s in the main diagonal. C will be an upper triangular matrix with integer entries and 1s in the main diagonal. This already implies that the equation $BCX = -U$ has a unique solution in X with integer entries. Since $X = -C^{-1}B^{-1}U$ we first define B in a way that we will have a clear description of $B^{-1}U$. $-B^{-1}U$ is the solution of the equation $-BZ = U$ where Z is an n by r matrix whose entries are variables. Let $\xi_1, ..., \xi_n$ be the rows of Z. If B is given, then using the fact that B is lower triangular we can determine the value of ξ_i by recursion on i. Each ξ_i will be a linear combination of the rows of $-U$ where the coefficients are determined by B. Since each row of U is an u_j, $j = 0, 1, ..., r-1$ or 0, we have that each ξ_i will be a linear combination of the vectors $u_0, ..., u_{n-1}$. Recall that the $j\mu$th row of U is u_j, for $j = 0, 1, ..., r-1$ and the other rows are 0. By definition the $j\mu$th row of B will contain a sigle 1 in the main diagonal and all of its other enries will be 0, that is, $b_{j\mu,j\mu} = 1$ and $b_{j\mu,k} = 0$ for all $j = 0, 1, ..., r-1$ and $k \neq j\mu$, where $B = \{b_{s,t}\}$. This implies that $\xi_{j\mu} = -u_j$ for $j = 0, 1, ..., r-1$. E.g. $\xi_0 = -u_0$. We want ot define B so that $\xi_2 = -ru_0, ..., \xi_j = -r^j u_0$ for $j = 0, 1, ..., \mu-1$. We can attain this if we put $b_{j,j-1} = -r$ for $j = 2, ..., m-1$ and $b_{j,t} = 0$ for all $t \neq j$, $t \neq j-1$, $j = 1, ..., \mu-1$. (That is the jth row will contain exactly two nonzero entries, in the main diagonal and immediately left from it.) Determining ξ_i by recursion on i we get the required values. The motivation for this definition is the following: as an integer linear combination of the integers $r^j u_0$, $j = 0, ..., r-1$ we can express any integer of the from bu_0 where b is a integer in the interval $[0, q) \subseteq [0, r^\mu)$. Therefore if we choose the further coefficients of B in a suitable way then we may force ξ_s for some $s > \mu$ take any value of the form bu_0. Since we want to do the same thing for $u_1, ...u_{r-1}$ as well we define the first $r\mu$ rows of B in the following way

$b_{i,i} = 1$ for all $0 = 1, ..., n-r-1$.

For all $j = \mu i + k$, $i = 0, ..., r-1$, $k = 1, ..., \mu-1$ we have $b_{j,j-1} = -r$.

All of the other entries in the first μr rows of B are 0.

The definition so far implied that

(B1) $\quad \xi_{i\mu+j} = -r^j u_i$ *for* $i = 0, ..., r-1$, $j = 0, ..., \mu-1$.

The next r rows, that is, rows $r\mu + k$, $k = 0, 1, ..., r-1$ have a special role. The definition of these rows will guarantee that

(B2) $\quad 2\xi_{r\mu+k} \equiv -u_k \pmod{q}$ *for* $k = 0, ..., r-1$.

To get this, first we take an integer z with $0 < z < q$ so that $2z \equiv 1 \pmod q$. Let

$$z = \sum_{s=0}^{\mu-1} \alpha_s r^s$$

where $0 \leq \alpha_s < r$ are integers for $s = 0, ..., \mu - 1$.

For all $j = \mu r + k$, $k = 0, ..., r-1$ and $i = 0, 1, ..., \mu - 1$ we put $b_{j,k\mu+i} = -\alpha_i$, and $b_{j,j} = 1$. All of the other entries of these rows are 0. This definition and (B1) implies (B2).

We want to define the remaining rows in a way that

(B3) *for any fixed $u_0, ..., u_{r-1}$, if $u_0, ..., u_{r-1}$ are linearly independent modulo q, then the distribution of $\xi_{(r+1)\mu}, \xi_{(r+1)\mu+1}, ..., \xi_{n-r-1}$ (with respect to the randomization of B), is uniform modulo q on the set of all r dimensional vector sequences of length $n - r - (r+1)\mu$.*

To attain this, first we define a random variable η whose values are sequences of integers $x_0, x_1, ..., x_{\mu-1}$ so that $0 \leq x_i < r$ for all $i = 0, ..., \mu - 1$, moreover we choose η so that the number $\sum_{i=0}^{\mu-1} x_i r^i$ has uniform distribution on the interval $[0, q-1]$. (Such an η can be efficiently generated by randomizing first the value of $\sum_{i=0}^{\mu-1} x_i r^i$ and then determining the unique values of the numbers x_i.)

Now we can define row j for all $j \geq (\mu+1)r$. For all $j \geq (\mu+1)r$ $b_{j,j} = 1$ for and $i = 0, ..., r-1$ the sequence of the entries $b_{j,\mu i}$, $b_{j,\mu i+1}$,...,$b_{j,\mu i+\mu-1}$ will be a random value of the random variable η. (For all of the possible numbers j the values of the random variable η are taken independently.) All of the other entries in these rows are 0.

(B1) and the definition of μ implies that for each $i \in [(r+1)\mu, n-r]$, ξ_i is the linear combination of the vectors $u_0, ..., u_{r-1}$, where the coefficients are taken at random and with uniform distribution modulo q, moreover these coefficients are independent for different values of i and for different elements of the sequence $u_0, ...,_{r-1}$. This implies (B3).

This completes the definition of B. We repeat the definiton below in a more concise form.

Definition of B. For the definition of B, first we define a random variable η whose values are sequences of integers $x_0, x_1, ..., x_{\mu-1}$ so that $0 \leq x_i < r$ for all $i = 0, ..., \mu - 1$. We choose η so that the number $\sum_{i=0}^{\mu-1} x_i r^i$ has uniform distribution on the interval $[0, q-1]$.

We will denote by $b_{i,j}$ the element of B in the ith row and jth column for $i = 0, ..., n-r-1$, $j = 0, ..., n-r-1$.

$b_{i,i} = 1$ for all $0 = 1, ..., n-r-1$.

For all $j = \mu i + k$, $i = 0, ..., r-1$, $k = 1, ..., \mu - 1$ we have $b_{j,j-1} = -r$.

For all $j = \mu r + k$, $k = 0, ..., r-1$ and $i = 0, 1, ..., \mu - 1$ we have $b_{j,k\mu+i} = -\alpha_i$ where $\sum_{s=0}^{\mu-1} \alpha_s (r)^s = z$, $0 \leq z < q$ and $2z \equiv 1 \pmod q$ and $0 \leq \alpha_s < r$ are integers for $s = 0, ..., \mu - 1$.

For all $j \geq (\mu+1)r$ and $i = 0, ..., r-1$ the sequence of the entries $b_{j,\mu i}$, $b_{j,\mu i+1}$,...,$b_{j,\mu i+\mu-1}$ will be a random value of the random variable η. (For all of the possible j and i the values of the random variable η are taken independently.)

All of the other entries of B are 0s.

The definition of C is simpler so we start with the formal definition.

Definition of C. $c_{i,j}$ will denote the jth element of the ith row in the matrix C for $i = 0, ..., n-r-1$, $j = 0, ..., n-r-1$.

$c_{i,i} = 1$ for all $i = 0, 1, ..., n-r-1$.

The entries $c_{i,j}$, $i \leq [\frac{n-r}{2}]$, $j > [\frac{n-r}{2}]$ are taken independently and with uniform distribution from the set $\{0, 1\}$.

All of the other entries of C are 0s.

Clearly we have that

(C1) C is an upper triangular matrix with 1's in the main diagonal.

This implies that we can compute the $(n-r-1-j)$th row of $C^{-1}(B^{-1}U)$ by recursion on j. Assume that the rows of the unique solution of $C^{-1}(-B^{-1}U)$ are the r-dimensional integer vectors $\rho_0, ..., \rho_{n-r-1}$.

Let $\kappa = [\frac{n-r}{2}]$. Since the rows of $B^{-1}U$ are $\xi_0, ..., \xi_{n-r-1}$ the definition of C implies that

(C2) $\rho_i = \xi_i$ *for all* $i = \kappa + 1, ..., n-r-1$.

and

(C3) $\rho_i = -\sum_{j=\kappa+1}^{n-r-1} c_{i,j}\rho_j = -\sum_{j=\kappa+1}^{n-r-1} c_{i,j}\xi_j$ for all $i = 0, 1, ..., \kappa$.

(The second equality is a consequence of (C2)). With a probability exponentially close to one for the randomization of $u_0, ..., u_{r-1}$, the sequence $u_0, ..., u_{r-1}$ is linearly independent modulo q. Assume now that such a sequence $u_0, ..., u_{r-1}$ is fixed. (B3) implies that the distribution of the sequence $\xi_\kappa, ..., \xi_{n-r-1}$ is uniform modulo q on the set of all sequences of length $n-r-1-\kappa$ consisting of r-dimensional vectors. Therefore we may apply Lemma A for the sum in (C3) so that I_q^r with the addition modulo q is the Abelian group. We get that

(C4') *for almost all fixed* $u_0, ..., u_{r-1}$, *and for allmost all fixed* $\xi_0, ..., \xi_{n-r-1}$ *(according to the distribution of B), the distribution of* $\rho_0, ..., \rho_\kappa$ *is almost uniform modulo q on the set of all r dimensional vector sequences of length* $\kappa + 1$.

More precisely we have the following:

(C4) *There is a* $c_4 > 0$ *so that for all sufficiently large n if we randomize* $u_0, ..., u_{r-1}$ *and B, then with a probability of at least* $1 - 2^{-c_4 n}$ *we get a sequence* $u_0, ..., u_{r-1}$, $\xi_\kappa, ..., \xi_{n-r}$, *so that for the randomization of C the distance of the distribution of the sequence* $\rho_0, ..., \rho_\kappa$ *from the uniform distribution is at most* $2^{-c_4 n}$.

This thogether with (C2) and (B3) implies that:

(C5) *There is a* $c_5 > 0$ *so that for all sufficiently large n and for the randomization of both B and C the distance of the distribtuion of the sequence* $\rho_0, ..., \rho_{n-r-1}$ *from the uniform distribtuion is at most* $2^{-c_5 n}$.

The definition of C also implies that every entry of C is small which will be useful when we estimate the length of the constructed linearly independent vectors. More precisely

(C6) *each entry of C in the main diagonal is* 1 *and all of the other entries belong to the set* $\{0, 2\}$.

Now we return to the equation $AY = 0$. The definitions of A_1, U, $\rho_0, ..., \rho_{n-r-1}$ imply that if S is an n by r matrix whose rows are $u_0, ..., u_{r-1}, \rho_0, ..., \rho_{n-r-1}$ then $AS = 0$. Therefore we may define the random lattice L by $u_{r+i} = \rho_i$ for $i = 0, ..., n-r-1$. That is, L is the set of integer vectors $h_0, ..., h_{n-1}$ with $\sum_{i=0}^{n-1} h_i u_i \equiv 0 \pmod q$. This definition together with (C6) implies that the distance of Γ_n and Φ_n is ineed at most 2^{-cn} for a suitably chosen constant $c > 0$ as claimed in the theorem. To complete the proof of the theorem we have to show only that using B and C we may construct n linearly independent elements of L each with length at most $n^2\sqrt{n}$.

$AS = 0$ implies that the rows of A are elements of L. They are clearly linearly independent since the submatrix $A_2 = BC$ has determinant 1. We have to construct r more linearly independent elements of L. We will add r new rows to the matrix A, the new matrix will be A'. The jth new row for some fixed $j = 0, ..., r-1$ is defined in the following way:

The $(n-r-1+j)$th row of A' is a sequence of length n that we get by the concatenation of the jth unit vector and the $(r\mu + j)$th row of C multiplied by two.

If we multiply this row by the matrix S then we get $u_j + 2(\rho_{r\mu+j} + \sum_{i=\kappa+1}^{n-r-1} c_{r\mu+j,i}\rho_i)$. By (C3) this is equal to $u_j + 2\xi_{r\mu+j}$. According to (B2) $2\xi_{r\mu+j} \equiv -u_j \pmod q$ and so the product is 0 modulo q. This shows that $A'S \equiv 0 \pmod q$ and so all of the rows of A' are elements of L. We have to prove that the rows are linearly independent (over the rationals). We show that the determinant of the matrix A' is an odd integer so it is not 0 which implies the required independence. Every element of A' is an integer (by definition of A'). We compute the determinant of A' modulo 2. A' consists of 4 submatrices A_1, A_2, A_3, A_4 where A_1, A_2 have been already defined; A_3 consist of those entries of A' which are in the last r rows and first r columns, A_4 consists of those entries of A' which are in the last r rows and last $n-r$ columns. Every entries of A_4 is even that is A_4 is zero modulo 2. Therefore the determinant of A' modulo 2 is equal to the products of the determinants of A_3 and A_2 modulo 2. A_3 is an r by r identity matrix so its determinant is 1. $A_2 = BC$. B is a lower triangular matrix C is an upper triangular matrix both have 1s in their main diagonal thefore the determinant of A_2 is 1. These imply that the determinant of A' is congruent to 1 modulo 2.

Finally we estimate the absolute values of the entries of A'. Each entry of A' outside A is $0, 1$ or 2. $A = BC$. The absolute value of each entry of C is ethier 0 or 1. Every entry of B is an integer in the interval $[0, r]$. Therefore each entry of A is an integer in the interval of $[-r(n-r), r(n-r)]$ and so this is true for the entries of A' as well. This implies that the Euclidean norm of our basis vectors is at most $(n(r(n-r))^2)^{\frac{1}{2}} = n^{\frac{1}{2}} r(n-r) \leq n^2\sqrt{n}$. (If we take into account that in each row of B the number of nonzero entries is relatively small, then we can improve this upper bound.)

References

1. M. Ajtai, Generating Hard Instances of Lattice Problems, Proceedings of the 28th Annual ACM Symposium on Theory of Computing, 1996, or Electronic Colloquium on Computational Complexity, 1996, http://www.eccc.uni-trier.de/eccc/
2. M. Ajtai and C. Dwork, A Public-Key Cryptosystem with Worst-Case/Average-Case Equivalence, Proceedings of the 29th Annual ACM Symposium on Theory of Computing, 1997, or
3. J-Y Cai, Some Recent Progress on the Complexity of Lattice Problems, Electronic Colloquium on Computational Complexity, 1999, http://www.eccc.uni-trier.de/eccc/, to appear in the Proceedings of the IEEE Conference of Computational Complexity, 1999.
4. J-Y Cai, A. Nerurkar. An Improved Worst-Case to Average-Case Connection for Lattice Problems. In Proc. 38th IEEE Symposium on Foundations of Computer Science, 1997, 468-477.
5. O. Goldreich, S. Goldwasser, S. Halevi, Collision-free hashing from lattice problems, Electronic Colloquium, on Computational Complexity, 1996, http://www.eccc.uni-trier.de/eccc/
6. O. Goldreich, S. Goldwasser, S. Halevi, Public-key cryptosystems from lattice reduction problems, In *Advances in Cryptology-Crypto'97*, Burton S. Kaliski Jr. (Ed.), Lecture Notes in Computer Science, 1294:112-131, Springer-Verlag, 1997.
7. O. Goldreich, S. Goldwasser, S. Halevi, Eliminating decryption errors in the Ajtai-Dwork cryptosystem, In *Advances in Cryptology-Crypto'97*, Burton S. Kaliski Jr. (Ed.), Lecture Notes in Computer Science, 1294:105-111, Springer-Verlag, 1997.