Combinatorics, Probability and Computing (1993) 2, 271–284

A Mildly Exponential Time Algorithm for Approximating the Number of Solutions to a Multidimensional Knapsack Problem

MARTIN DYER[†], ALAN FRIEZE[‡], RAVI KANNAN[‡],
AJAI KAPOOR[‡], LJUBOMIR PERKOVIC[‡] and UMESH VAZIRANI[§]

[†]University of Leeds, Leeds LS2 9JT, UK

[‡]Carnegie Mellon University, Pittsburgh PA15213, USA

[§]University of California, Berkeley CA94320, USA

Received 5 November 1992; revised 12 May 1993

For Paul Erdős on his 80th birthday

We describe a $2^{O(r\sqrt{n}(\log n)^{5/2})}\epsilon^{-2}$ time randomized algorithm that estimates the number of feasible solutions of a multidimensional knapsack problem within $1 \pm \epsilon$ of the exact number. (Here r is the number of constraints and n is the number of integer variables.) The algorithm uses a Markov chain to generate an almost uniform random solution to the problem.

1. Introduction

An instance of the multidimensional knapsack problem in n variables is defined by a non-negative $r \times n$ integer matrix A, a vector $d \in \mathbb{Z}^n$, and a vector $b \in \mathbb{Z}^r$. We assume, to avoid trivialities, that all components of b and d are positive. The set of feasible solutions K is then

$$K = \{x \in \mathbb{Z}^n \mid Ax \le b,\ 0 \le x \le d\}. \tag{1}$$

We will assume, without loss of generality, that $d_j \le \min_i b_i/a_{ij}$. Let $d_{\max} = \max_j d_j$. In particular, if $d_{\max} = 1$, we have the *zero-one* multidimensional knapsack problem, and if $r = 1$ we have the knapsack problem. The *optimization* problem consists of finding the maximum value of a given linear function over K. This is known to be NP-complete, even for $r = 1$ and zero-one variables. The *counting* problem seems to be even harder. This asks for $|K|$. This problem is #P-complete, again even for $r = 1$ and zero-one variables.

Markov chains have been successfully used to approximately solve several #P-complete problems [1, 2, 3, 4, 6, 7, 10, 12, 14]. In all of these problems the running time of the algorithm is polynomial in problem size and relative error. On the other hand, the general zero-one permanent still resists polynomial time approximation, though Jerrum

Vazirani [9] have reduced the time complexity to $2^{O(\sqrt{n}(\log n)^2)}\epsilon^{-2}$ for computing an roximation, *i.e.* an approximation with relative error in the range $1 \pm \epsilon$.

this paper we make similar progress in approximating $|K|$. We show that there is a $\overline{n}(\log n)^{5/2})\epsilon^{-2}$ time algorithm for computing an ϵ-approximation to $|K|$. Furthermore, $d_j \geq n^2$ for $j \in [n] = \{1, 2, \dots, n\}$, we can make the scheme polynomial.

te that there is an easy randomized approximation algorithm, given by generating om points as follows. Suppose we simply choose x_j randomly in $[0, d_j]$. It is obvious

$$\Pr(x_j \leq \lfloor d_j/n \rfloor) \geq 1/(2n).$$

ever, if $x_j \leq \lfloor d_j/n \rfloor$ $(j \in [n])$, we have

$$Ax \leq \tfrac{1}{n} Ad \leq b,$$

$a_{ij}d_j \leq b_i$ for all $i \in [r]$, $j \in [n]$. Therefore $x \in K$. Thus, by randomly generating x in ashion, we have probability $(2n)^{-n}$ of having $x \in K$. Hence, a uniformly distributed in K can be generated in $(2n)^{n+1}$ time with very high probability. This easily gives proximation algorithm with the time complexity $n^{O(n)}r\epsilon^{-2}$. As previously stated, our ximation algorithm runs in time $2^{O(r\sqrt{n}(\log n)^{5/2})}$, so we will assume here that $r = O(n^\kappa)$ me fixed $\kappa < \frac{1}{2}$. (In the zero-one case, an $O(rn2^n)$ time *exact deterministic* algorithm course, trivial.) It may be worth pointing out that while there are fully polynomial approximation schemes for the optimisation version of the knapsack problem, there one for the multidimensional problem unless P=NP. Furthermore, we have not been o make any use of these optimisation results for knapsack in the associated counting em.

develop the argument in three steps. First we examine the zero-one knapsack em in Section 3, then move to the general zero-one case in Section 4. Finally, we der the general problem in Section 5.

a tool in our proof, we prove a general fact about random sampling (Theorem 7.2) may be of independent interest, so we shall mention it here: suppose we have a lation of n non-negative reals $c_1, c_2, \dots, c_n$ with mean μ and $c_i \leq \alpha$, for $i = 1, 2, \dots, n$, we pick without replacement a sample of t c_i's; let S_t be their sum. The Chernoff-ding Theorems assert

$$\Pr(S_t - t\mu \geq x) \leq \exp\left\{-\frac{2x^2}{t\alpha^2}\right\} \qquad \text{for all } x \geq 0.$$

rove a similar bound, but with α replaced by a quantity that we have 'observed' from amples. Let S_m be the sum of the m largest samples among the t we have picked. we prove

$$\Pr(S_t - t\mu > S_m) = O(\exp\{-m^2(t-m)^2/t^3\}) \qquad \text{for } t = m+1, \dots, n.$$

2. Rapidly mixing Markov chains

well known that the approximate counting of combinatorial objects is intimately d to their near uniform generation – see Jerrum, Valiant and Vazirani [8] for a l statement of this relation.

In our problem this general reduction implies that if in time $T(n)$ we can generate a solution $x \in K$ with probability $p(x)$ so that, say, $p(x)/p(y) \leq 2$ for all $x, y \in K$, then it takes $O(T(n)s(n)\epsilon^{-2}\log\delta^{-1})$ time to compute an ϵ-approximation with probability at least $1 - \delta$, where $s(n)$ is a polynomial in n. As our $T(n)$ dominates the remaining terms, we concentrate on estimating its value from now on.

For this purpose we define an ergodic reversible Markov chain with set of states K whose steady state distribution is uniform. We then run this chain for a sufficient number of steps that we can be sure we are close enough to the steady state. We then take the current state as our near uniform sample.

In detail, let K be the set of states of Markov chain $\mathcal{M}$. If $x, y \in \mathbb{Z}^n$, define the Hamming distance $h(x,y) = |\{j : x_j \neq y_j\}|$. (Normally this is defined only for zero-one vectors, and this will be the principal use here, but we also use the definition for general integer vectors.) The transition probabilities $p(x,y)$ are then given by

$$p(x,y) = \begin{cases} 0 & \text{if } h(x,y) > 1 \\ \frac{1}{2nd_{\max}} & \text{if } h(x,y) = 1 \\ 1 - \sum_{z \neq x} p(x,z) & \text{if } y = x. \end{cases}$$

Note that $\mathcal{M}$ can be simulated easily, as follows. Start at any point of K (*e.g.* the origin). At the 'current' point $x \in K$, repeat the following step. Do nothing with probability $\frac{1}{2}$, otherwise choose a coordinate direction $k \in [n]$ uniformly at random. Choose an integer $x'_k \neq x_k$ from $[0, d_{\max}]$ uniformly at random. Let $x'_j = x_j$ $(j \in [n] \setminus \{k\})$. If $x' \in K$, x' becomes the new current point, otherwise remain at x. Note also that since $\mathcal{M}$ is symmetric, aperiodic and irreducible, its stationary distribution π is uniform over its states.

Now let $p^{(t)}$ be the distribution of the current point after t steps starting at $x = 0$. The variational distance between $p^{(t)}$ and π can be bounded in terms of the *conductance* Φ:

$$\Phi = \min\left\{\Phi_S : \pi(S) \leq \tfrac{1}{2}\right\},$$

where for $S \neq \emptyset$,

$$\Phi_S = \frac{\sum_{x \in S, y \in \bar{S}} \pi(x)p(x,y)}{\pi(S)},$$

and

$$\pi(S) = \sum_{x \in S} \pi(x).$$

It will be useful to think in terms of a digraph $\Gamma = (K, E)$, where $E = \{(x,y) \in K^2 : h(x,y) = 1\}$. If we let $E_{S:\bar{S}} = \{(x,y) \in E : x \in S, y \notin S\}$ and $\rho(S) = |E_{S:\bar{S}}|/|S|$, then

$$\Phi = \min_{|S| \leq N/2} \left\{\frac{\rho(S)}{2nd_{\max}}\right\} \tag{2}$$

Now, letting $N = |K|$, it follows from results in Sinclair and Jerrum [15] that for all $x \in K$

$$|p^{(t)}(x) - \pi(x)| \leq \sqrt{N}(1 - \Phi^2/2)^t.$$

Thus our claim about near uniform generation can be justified by showing that the nductance Φ of $\mathscr{M}$ satisfies

$$\Phi = 2^{-O(r\sqrt{n}(\log n)^{5/2})}. \tag{3}$$

view of (2), assuming that $d_{\max}$ is suitably bounded as a function of n, this will then low from

$$\rho(S) = 2^{-O(r\sqrt{n}(\log n)^{5/2})} \qquad \text{for all } S \subseteq K, |S| \le N/2. \tag{4}$$

will use a variation of the canonical path argument introduced by Jerrum and clair [6]. Fix $S \subseteq K, |S| \le N/2$. We will define a set $T = T(S) \subseteq S \times \bar{S}$ with

$$|T| \ge \frac{|S| \cdot |\bar{S}|}{2}. \tag{5}$$

will also define a *canonical* path $P_{x,y}$ in Γ from x to y for every $(x, y) \in T$. For each $w) \in E_{S:\bar{S}}$, we let $W_{v,w}$ denote the set of canonical paths using the edge (v, w). Let $_{,} = |W_{v,w}|$ and let $\lambda = \lambda(S) = \max\{\lambda_{v,w} : (v, w) \in E_{S:\bar{S}}\}$. Clearly

$$\begin{aligned} |E_{S:\bar{S}}| &\ge \frac{|T|}{\lambda} \\ &\ge \frac{|S| \cdot |\bar{S}|}{2\lambda}, \end{aligned}$$

$$\rho(S) \ge \frac{N}{4\lambda}.$$

will complete the proof of (4) by showing that for any S

$$\lambda = 2^{O(r\sqrt{n}(\log n)^{5/2})}N. \tag{6}$$

3. The zero-one knapsack problem

concentrate first on the zero-one case. The case $r = 1$ has a special feature that allows lightly simpler proof. We will give this, and then analyse the general zero-one case later. r simplicity of notation we now let $K = \{x \in \{0, 1\}^n : a_1x_1 + a_2x_2 + \cdots + a_nx_n \le b\}$, ere $a_1, a_2, \ldots, a_n, b$ are positive integers.

fining canonical paths

onsider a permutation σ on $[n]$, an *offset* u $(0 \le u < n)$, and states $x \in S$ and $y \in \bar{S}$. We fine the sequence $Q_{x,y} = Q_{x,y}(\sigma, u) = v^0, v^1, \ldots v^n$ as follows: $v^0 = x, v^n = y$, and $v^i_j = v^{i-1}_j$ $j \ne \sigma(i \oplus u)$ and $v^i_{\sigma(i\oplus u)} = y_{\sigma(i\oplus u)}$, $i \oplus u = (i + u - 1 \bmod n) + 1$. Thus, we go through components of x in the order $\sigma(1 \oplus u), \sigma(2 \oplus u), \ldots, \sigma(n \oplus u)$, changing one component om x_j to y_j at each step. If all intermediate points are in K, we say $Q_{x,y}$ is feasible. (We ay remove the loops caused by $v^i = v^{i+1}$.)

Assume we have chosen σ, u, and for notational convenience assume that σ is the entity permutation and $u = 0$. Fix $(v, w) \in E_{S:\bar{S}}$ and consider those $(x, y) \in S \times \bar{S}$ for nich the path $Q_{x,y}$ uses (v, w). Then, for some $t \ge 1$, we can write

$$v = (y_1 \ldots y_{t-1}x_tx_{t+1} \ldots x_n) \quad \text{and} \quad w = (y_1 \ldots y_{t-1}y_tx_{t+1} \ldots x_n).$$

nen σ, u, and (v, w) together fix $y_1, \ldots, y_t$ and $x_t, \ldots, x_n$, and $\lambda_{v,w}$ is bounded by the number

of possibilities for $x_1, \ldots, x_{t-1}, y_{t+1}, \ldots, y_n$. This leads to the idea of the *complementary point* $w' = (x_1, \ldots, x_t, y_{t+1}, \ldots, y_n)$ of (v, w) from Jerrum and Sinclair [15]. Let $W' = W'(x, y)$ be the set of complementary points w' such that (v, w) is on $Q_{x,y}$. Clearly, if we use the same σ for each x, y, then the number of (x, y) pairs in $S \times \bar{S}$ for which $Q_{x,y}$ uses (v, w) is at most n times the total possible number of complementary points for (v, w). (Since n is the number of choices for u.)

Now let $D_\beta = \{\xi : h(\xi, \eta) \le \beta \text{ for some } \eta \in K\}$. Then, the following lemma holds:

Lemma 3.1. *There exist σ^* and $T^* \subset S \times \bar{S}$ such that $|T^*| \ge \frac{|S||\bar{S}|}{2}$ and*

(i) $W' \subseteq D_{4m}$, where $m = \lceil 4\sqrt{n \log_2 n}\rceil$.
(ii) For all $(x, y) \in T^*$, there exists $u^* = u^*(x, y)$ such that $P_{x,y} = Q_{x,y}(\sigma^*, u^*)$ is feasible.

Proof. Fix $x \in S$, $y \in \bar{S}$. Choose σ randomly, u arbitrarily and an intermediate point v of $Q_{x,y}$, say the ℓ-th point in the sequence. For $\eta \in \{0, 1\}^n$, let its support $I_\eta = \{j : \eta_j = 1\}$. Let $I = \{\sigma(1 \oplus u), \sigma(2 \oplus u), \ldots, \sigma(\ell \oplus u)\}$. Then

$$I_{w'} = (I_x \cap I) \cup (I_y \setminus I),$$

where w' is the complementary point corresponding to the edge (v, w) of $Q_{x,y}$ that starts with v.

Now, for $X \subseteq [n]$, let $a(X) = \sum_{j\in X} a_j$. Then $a(I_x \cap I)$ is the sum of the elements of a random ℓ-subset of the *multiset* $A_x = \{a_jx_j : j \in [n]\}$. Assume next that $|I_x \cap I| \ge 2m$, and let Δ_x denote the sum of the m largest elements of the multiset $\{a_j : j \in I_x \cap I\}$. Now, if $ax = \sum_{j\in[n]} a_jx_j$,

$$E(a(I_x \cap I)) = \mu_x = \frac{\ell}{n}ax,$$

so from Theorem 7.2 (see Section 7),

$$\begin{aligned} \Pr(a(I_x \cap I) \ge \mu_x + \Delta_x) &= O(e^{-m^2/4\ell}) \\ &= O(n^{-4}). \end{aligned}$$

Thus, regardless of the size of $I_x \cap I$, we can assert that with probability $1 - O(n^{-4})$ ther exists a set $J_x \subseteq I_x \cap I$ such that

$$|(I_x \cap I) \setminus J_x| \le 2m \qquad (7$$

$$a(J_x) \le \mu_x. \qquad (8$$

Now consider $I_y \setminus I$.

$$E(a(I_y \setminus I)) = \mu_y = \frac{n - \ell}{n}ay.$$

Then, in an analogous fashion to $I_x \cap I$, we have that with probability $1 - O(n^{-4})$ the exists a set $J_y \subseteq I_y \setminus I$ such that

$$|(I_y \setminus I) \setminus J_y| \le 2m \qquad ($$

$$a(J_y) \le \mu_y. \qquad (1$$

define w'' by $I_{w''} = J_x \cup J_y$. Then (7) and (9) imply

$$h(w', w'') \le 4m.$$

that $w'' \in K$. Indeed, using (8) and (10)

$$\begin{aligned} aw'' &= a(J_x) + a(J_y) \\ &\le \frac{\ell}{n}ax + \frac{n-\ell}{n}ay \\ &\le \frac{\ell}{n}b + \frac{n-\ell}{n}b \\ &= b. \end{aligned} \tag{11}$$

ach of the pairs (x, y) such that $x \in S$ and $y \in \bar{S}$, we have that the probability a
permutation satisfies

$$w' \in D_{4m} \text{ for all complementary points } w' \text{ arising from all offsets} \tag{12}$$

st $1 - O(1/n^2)$. Then by a simple counting argument we have that there must exist
rmutation σ^* with at least a $1 - O(1/n^2)$ fraction of x, y pairs satisfying (12).
ach x, y there is an offset $u^* = u^*(x, y)$ such that $Q_{x,y}(\sigma^*, u^*)$ is feasible (see
[11], Problem 3.21 – the *gas station* problem). Thus there exists a set $T^* \subseteq S \times \bar{S}$
at

$$|T^*| \ge |S| \cdot |\bar{S}|(1 - O(n^{-2})), \tag{13}$$

$= Q_{x,y}(\sigma^*, u^*)$ is feasible for all $(x, y) \in T^*$. This completes the proof of the
□

ly observe that for $(v, w) \in E_{S:\bar{S}}$ we have

$$\begin{aligned} \lambda_{v,w} &\le n|D_{4m}| \\ &\le nN\binom{n}{4m} \\ &= 2^{O(\sqrt{n}(\log n)^{3/2})}N, \end{aligned}$$

follows immediately.

4. The general zero-one problem

≥ 2 the argument that the complementary points are almost always 'close' to K
alid, but it is no longer possible to use an offset to make the intermediate points
satisfy all the constraints simultaneously. Since offsets are no longer in use, we
e associated parameter in $Q_{x,y}$.
$R \subseteq [n]$ and $x \in \{0,1\}^n$, we define $z = z(x, R)$ by $I_z = I_x \setminus R$, *i.e.* to obtain z, simply
ponents j to zero for $j \in R$.
n $x, y \in K$, permutation σ and $R \subseteq J(x, y) = (I_x \setminus I_y) \cup (I_y \setminus I_x)$, we define a
rmutation $\tau = \tau(x, y, \sigma, R)$ and then take $Q_{x,y}(\tau)$ as our path. Here τ is defined
ws: let $R_\alpha = R \cap I_\alpha$ and $r_\alpha = |R_\alpha|$ for $\alpha = x, y$. Starting with the sequence
$\sigma(1), \sigma(2), \ldots, \sigma(n)$, we move the elements of R_x to the front (in natural order), and then move the elements of R_y to the back. τ is defined by the sequence obtained. For example, if $\sigma = (10, 9, 1, 3, 7, 4, 8, 5, 6, 2)$ and $R_x = \{7, 9\}, R_y = \{3, 5\}$, then $\tau = (7, 9, 10, 1, 4, 8, 6, 2, 3, 5)$.

Lemma 4.1. *There exists σ^* and $T^* \subseteq S \times \bar{S}$ such that $|T^*| \ge \frac{|S||\bar{S}|}{2}$ and*

(i) $W' \subseteq D_{16mr\log_2 n + 4mr}$, $\qquad (m = \lceil 4\sqrt{n \log_2 n}\rceil)$

(ii) For all $(x, y) \in T^*$, there exists $R = R(x, y), |R| \le 16mr\log_2 n$ such that $Q_{x,y}(\tau)$ is feasible.

Proof. Fix $x \in S$, $y \in \bar{S}$ and choose σ randomly. Observe first that no matter what choice we make for R, it is the case that each complementary point of $Q_{x,y}(\tau)$ is within Hamming distance $|R|$ of a complementary point of $Q_{x,y}(\sigma)$. Consider a complementary point w' of $Q_{x,y}(\sigma)$. The analysis of Lemma 3.1 shows that with probability $1 - O(r/n^4)$ we can find sets $X_1, X_2, \ldots, X_r$ all of size at most $4m$ such that zeroising the X_i-components of w' produces a vector satisfying the ith constraint (here X_i is equal to $J_x \cup J_y$ of the lemma). Hence zeroising all of the $\bigcup_{i=1}^r X_i$-components produces a member of K. Thus, in this case all complementary points of $Q_{x,y}(\tau)$ are within Hamming distance $|R| + 4mr$ of K, and the first part follows (modulo a definition of R).

Our next observation is that if

$$R' \subseteq R \subseteq J(x, y),$$

and all intermediate points in $Q_{x,y}(\tau(x, y, \sigma, R'))$ satisfy the ith constraint, the same is true for $Q_{x,y}(\tau(x, y, \sigma, R))$. This is simply because the intermediate points in the latter path have supports that are subsets of those in the former.

We will now define $R = R_1 \cup R_2 \cup \cdots \cup R_r$, where all we claim is that the intermediate points of $Q_{x,y}(\tau(x, y, \sigma, R_i))$ satisfy the ith constraint with probability $1 - O(\log_2 n/n^4)$.

We will now concentrate on R_1, which we decompose as $\bigcup_{j=1}^p R_{1,j}$, where $p \le \log_2 n$. We will use the notation $a^1(I) = \sum_{j \in I} a_{1j}$ for $I \subseteq [n]$.

Let v be one of the first $n/2$ points of $Q_{x,y}(\sigma)$. Let $B_x = I_v \cap (I_x \setminus I_y)$ and $B_y = I_v \cap (I_y \setminus I_x)$ so that $I_v = B_x \cup B_y \cup (I_x \cap I_y)$. We can argue, as in the proof of Lemma 3.1, that with probability $1 - O(n^{-4})$ there exist $B''_x \subseteq B_x, B''_y \subseteq B_y$ with $|B_x - B''_x|, |B_y - B''_y| \le 2m$ and $a^1(I_{v''}) \le b_1$, where $I_{v''} = B''_x \cup B''_y \cup (I_x \cap I_y)$. If $|I_x \setminus I_y| > 8m$, then L_x is the index set of the $8m$ largest elements in $I_x \setminus I_y$. Otherwise $L_x = I_x \setminus I_y$. Define L_y similarly with respect to $I_y \setminus I_x$. It follows from Theorem 7.1 (below) that if $|L_x| \ge 8m$, then $|L_x \cap I_v| \ge 2m$ with probability $1 - O(n^{-4})$. (An element of L_x is in I_v with probability at least one half.) Similarly, $|L_y| \ge 8m$ implies $|L_y \cap I_v| \ge 2m$ with probability $1 - O(n^{-4})$. Hence with high probability, if $\tilde{v}$ is defined by $I_{\tilde{v}} = I_v \setminus (L_x \cup L_y)$, then $a^1(I_{\tilde{v}}) \le a^1(I_{v''}) \le b_1$.

Thus with probability $1 - O(n^{-4})$, the first $n/2$ points of $Q_{x,y}(\tau(x, y, \sigma, L_x \cup L_y))$ satisfy the first inequality. We therefore take $R_{1,1} = L_x \cup L_y$. Let x' denote the $\frac{1}{2}n$th point of $Q_{x,y}(\tau(x, y, \sigma, L_x \cup L_y))$, and condition on its value. The remaining $n/2$ components are changed by σ in random order in going from x' to y. To define $R_{1,2}$, repeat the above argument with x' in place of x, and $n/4$ in place of $n/2$. In this way we obtain a set $R_{1,2}$ such that with probability $1 - O(n^{-4})$, the first $3n/4$ points of $Q_{x,y}(\tau(x, y, \sigma, R_{1,1} \cup R_{1,2}))$

sfy the inequality. The remaining sets in the partition of R_1 are obtained similarly. We stop when we have at most $16m$ components to change in order to get to y.
he existence of T^* is now inferred as at the end of the proof of Lemma 3.1. □

Ve can now prove (6) fairly easily. Fix $(v, w) \in E_{S:\bar{S}}$. If $Q_{x,y}$ uses (v, w), we can fix x, y by ng the permutation τ and the complementary point. But there are at most $\binom{n}{16mr\log_2 n}$ ices for τ, given σ^*. Hence,

$$\begin{aligned} \lambda_{v,w} &\leq n|D_{16mr\log_2 n+4mr}|\binom{n}{16mr\log_2 n} && (14)\\ &\leq n\binom{n}{16mr\log_2 n+4mr}N\binom{n}{16mr\log_2 n} && (15)\\ &= 2^{O(r\sqrt{n}(\log n)^{5/2})}N, && (16)\end{aligned}$$

(6) follows immediately.

5. The general problem

now consider the general case (1). Observe from (2) that Φ will be very small if $d_{\max}$ ery large. Note also that the commonly used device of replacing a general integer able x_j by a sum of zero-one variables $\sum_{s=0}^{\ell_j} 2^s z_{sj}$, where ℓ_j is suitably chosen, does seem to work here for two reasons:

If $d_j \neq 2^{\ell_j+1} - 1$, the number of solutions is not preserved (unless we add a further constraint).

The number of variables n is increased by a factor $\sum_j \log_2(d_j + 1)$. If any d_j is nonpolynomially large in n, this leads to a significant increase in the algorithm's time complexity.

s we will adopt a different strategy. We need to be able to deal with the possibility ery large d_j, but first consider the case where $d_{\max} < n^3$. If canonical paths and plementary points are defined exactly as before, the arguments of Section 4 require minor modification.

hus, given $x, y \in K$, consider two zero-one vectors $\xi^{(1)}$, $\xi^{(2)}$, where $\xi_j^{(1)} = 1$, $\xi_j^{(2)} = 0$ $> y_j$, and $\xi_j^{(1)} = 0$, $\xi_j^{(2)} = 1$ if $y_j > x_j$. (If $x_j = y_j$, the values of $\xi_j^{(1)}$, $\xi_j^{(2)}$ can be trary.) Now, the canonical path from x to y can be chosen using that from $\xi^{(1)}$ to $\xi^{(2)}$ ne zero-one polytope defined by the system

$$\sum_{j=1}^{n}(a_{ij}|x_j - y_j|)\xi_j \leq (b_i - \sum_{j=1}^{n} a_{ij}\min\{x_j, y_j\}) \quad (i \in [r]),$$

re x, y are to be treated as constant vectors. We simply interpret changing a component $\xi_j^{(1)}$ to $\xi_j^{(2)}$ as requiring the change of a component from x_j to y_j. We can apply ma 4.1 to this system and the bound on Hamming distance still applies. Now the ber of points within Hamming distance β of K is clearly at most $n^{3\beta}$ times the nate (15). This additional factor does not, however, inflate the estimate (16).
 finish this case we must check that the intermediate points of the path $Q_{x,y}$ so defined are feasible. Consider the kth point and for notational convenience assume that $\tau = (1, 2, \ldots, n)$. Then we know that

$$\sum_{i=1}^{k}((a_{ij}|x_j - y_j|)\xi_j^{(2)} + \sum_{j=k+1}^{n}(a_{ij}|x_j - y_j|)\xi_j^{(1)} \leq (b_i - \sum_{j=1}^{n} a_{ij}\min\{x_j, y_j\}) \quad (i \in [r]).$$

But

$$\min\{x_j, y_j\} + |x_j - y_j|\xi_j^{(2)} \geq y_j$$

and

$$\min\{x_j, y_j\} + |x_j - y_j|\xi_j^{(1)} \geq x_j.$$

Thus,

$$\sum_{i=1}^{k} a_{ij}y_j + \sum_{j=k+1}^{n} a_{ij}x_j \leq b_i \quad (i \in [r]),$$

and the path $Q_{x,y}$ is feasible. Thus we may conclude that (6) remains valid when $d_{\max} < n^3$ (and, in fact, for any polynomial bound on $d_{\max}$).

Thus suppose, for some k $(0 \leq k < n)$, that $d_j < n^3$ for $j = 1, 2, \ldots, k$, and $d_j \geq n^3$ for $j = k+1, k+2, \ldots, n$. Define $\sigma_j = \lceil (d_j + 1)/n^3 \rceil$, and let $x_j' = \lfloor x_j/\sigma_j \rfloor$, $d_j' = \lfloor d_j/\sigma_j \rfloor$ for $j \in [n]$. Also let $a_{ij}' = \sigma_j a_{ij}$ for $i \in [r]$, $j \in [n]$. We can generate a point (near) uniformly in $K' = \{x' \in \mathbb{Z}^n : A'x' \leq b, 0 \leq x' \leq d'\}$ by the above method, since

$$d_j' \leq d_j/\sigma_j \leq n^3 d_j/(d_j + 1) < n^3.$$

After generating such an x', we then choose x by

$$x_j = \sigma_j x_j' + Z_j, \quad (j \in [n]), \tag{17}$$

where Z_j is an integer chosen uniformly from $[0, \sigma_j - 1]$. We accept the point x if it lies in K, otherwise we try again. Now (17) determines a bijection between the integer x's in some set H and the pairs (x', Z). The generated x's are evidently uniform on H, a union of hyper-rectangles, one corresponding to each x'. Note that $K \subseteq H$, since for each $x \in K$ there is a unique pair (x', Z) with $x' \in K'$ given by $x_j' = \lfloor x_j/\sigma_j \rfloor$, $Z_j = x_j \bmod \sigma_j$, $j \in [n]$ The accepted points will, therefore, be (near) uniform in K, as required. However, th generated x may be rejected, so we must check that acceptance occurs with sufficiently higl probability. It is clearly enough that the acceptance probability be large in comparisoı with the estimate of conductance (3). In that case the number of repetitions required fo acceptance will not significantly affect the total time to generate a (near) uniform poin in K.

Suppose we have some 'good' set $G \subseteq K'$ such that

(i) $\Pr(x \in K \mid x' \in G) \geq \frac{1}{2}$,
(ii) $\Pr(x' \in G) \geq n^{-4r}$.

Then it is easy to see that

$$\Pr(x \in K) \geq \Pr(x \in K \mid x' \in G)\Pr(x' \in G) \geq \tfrac{1}{2}n^{-4r},$$

which is large compared to (3), and we are done.

s it remains only to define the set G and prove that it has properties (i) and (ii). To d, for $y \in \mathbb{R}^n$, let $y = (\hat{y}, \bar{y})$, where $\hat{y} \in \mathbb{R}^k$, $\bar{y} \in \mathbb{R}^{n-k}$, and k is as defined above. We e the same notation for the corresponding partition of a matrix by its first k and $-k$ columns. Note that $\hat{x} = \hat{x}'$, $\hat{A} = \hat{A}'$, since $\sigma_j = 1$ for $j \le k$. Now define

$$G = \{x' \in K' : \hat{A}\hat{x} \le \tfrac{k}{k+1}b\} \text{ and } \hat{G} = \{\hat{x'} : x' \in G\}.$$

5.1. $\Pr(x \in K \mid x' \in G) \ge \frac{1}{2}$.

For $x \in H$ let

$$D(x) = \{y \in \mathbb{R}^{n-k} : x_{k+j}/\sigma_{k+j} \le y_j < (x_{k+j}+1)/\sigma_{k+j},\ (j \in [n-k])\}.$$

$\in \hat{G}$. Clearly $(\hat{g}, \xi) \in K'$ if and only if ξ lies in the polytope

$$\bar{P} = \{\xi \in \mathbb{R}^{n-k} : \bar{A}'\xi \le b - \hat{A}\hat{g} = b^*, 0 \le \xi \le \bar{d}'\},$$

$^* \ge \frac{1}{k+1}b$. Now

$$\Pr(x \in K \mid \hat{x}' = \hat{g}) = \frac{\mathrm{vol}\,(H')}{\mathrm{vol}\,(H'')}, \tag{18}$$

$$H' = \bigcup_{\substack{x \in K \\ \hat{x}' = \hat{g}}} D(x) \text{ and } H'' = \bigcup_{\substack{x \in H \\ \hat{x}' = \hat{g}}} D(x).$$

$\supseteq \bar{P}$, since if $\xi \in \bar{P}$, then $\xi \in D(x)$, where $\hat{x} = \hat{g}, x_{j+k} = \lfloor \sigma_{j+k}\xi_{j+k} \rfloor$ for $j \in [n-k]$ s a member of K.

e other hand, the assumptions on d_j imply

$$a'_{ij} \le a_{ij}(2d_j/n^3) \le 2b_i/n^3 \le 2(k+1)b^*_i/n^3. \tag{19}$$

n $z \in H''$ implies

$$\bar{A}'z \le b^* + \bar{A}'\mathbf{1} \le (1 + \tfrac{2(k+1)(n-k)}{n^3})b^*,$$

is the vector of all 1's, using (19). So

$$H'' \subseteq \left(1 + \frac{2(k+1)(n-k)}{n^3}\right)\bar{P}. \tag{20}$$

$$\Pr(x \in K \mid \hat{x}' = \hat{g}) \ge (1 + \tfrac{2(k+1)(n-k)}{n^3})^{-(n-k)} \ge \exp\{-2(k+1)(n-k)^2/n^3\} \ge \tfrac{1}{2},$$

4, completing the proof. □

5.2. $\Pr(x' \in G) \ge n^{-4r}$.

If $x' \in K' \setminus G$, consider the rows $i \in [r]$ such that $(\hat{A}\hat{x})_i > \frac{k}{k+1}b_i$. For each such exists a smallest $t = t(i)$ $(1 \le t \le k)$ such that $a_{it}x_t > b_i/(k+1)$. Thus define a

function $g : K' \to G$ by

$$g_j(x') = \begin{cases} x'_j & \text{if } j \ne t(i) \text{ for any } i, \\ 0 & \text{otherwise.} \end{cases}$$

Clearly $g(x') \in G$, as required. Since $g(x')$ differs from x' in at most $\min\{r,k\}$ coordinates, the point-to-set map g^{-1} clearly partitions K' into classes of size at most

$$\binom{n}{r} n^{3\min\{r,k\}} \le n^{4r},$$

since $x' < n^3\mathbf{1}$. Hence $|K'| \le n^{4r}|G|$ and

$$\Pr(x' \in G) = |G|/|K'| \ge n^{-4r},$$

as claimed. □

6. A polynomially solvable case

In this section we prove a stronger result in a special case. If $d_j \ge n^2, j = 1, 2, \ldots, n$, we can construct a *fully polynomial* randomized approximation scheme for $|K|$, *i.e.* our algorithm is polynomial in n, ϵ^{-1}. Thus such cases are 'easy', since the counting closely resembles volume computation [4].

We can use the scaling of the previous section to 'round' the feasible polytope K to K'. Then we have $B(n/2) \subseteq K' \subset B(n^3)$, where $B(v) = \{0 \le x' \le v\mathbf{1}\}$. The first inclusion follows from $a_{ij}\sigma_j \le 2a_{ij}d_j/n^2 \le 2b_i/n^2$ for $j \in [n]$, while the second is a restatement of $d'_j < n^3$. We perform a *biased* random walk on the integer lattice points $x' \in B(n^3)$ with the weighting function $T(x') = e^{-2nt(x')}$, where

$$t(x') = \min\{t \ge 0 : A'x' \le (1+t)b\}.$$

At a point x' we do nothing with probability 1/2. Otherwise we randomly choose $\pm j$ from $\{\pm 1, \pm 2, \ldots, \pm n\}$. We then let $y' = x' \pm e_j$, where e_j denotes the jth unit vector. If $y' \in B(n^3)$, we move there with probability $\min\{1, T(y')/T(x')\}$. This completes a step of the walk.

It is easily shown that t varies by only a constant factor over any unit cube in $B(n^3)$, using the rounding property. Indeed, if $A'x' \le (1+t)b$,

$$A'(x' + \mathbf{1}) \le \left(1 + t + \frac{2}{n}\right)b. \tag{21}$$

Walks of this type were studied in Applegate and Kannan [1] (see also Dyer and Frieze [3] or Lovász and Simonovits [13] for some improvements). The function T is log-concave and $\log T$ has a Lipschitz constant of $O(n)$. It follows that the walk mixes rapidly, *i.e.* the conductance is $1/p(n)$ for some polynomial p, and we can obtain a near uniform random point in K' in polynomial time.

A point x is generated from a random $x' \in K'$ as in the previous section – see (17).

nding property ensures a probability of at least e^{-2} that $x \in K$.

$$\begin{aligned} \Pr(x \in K) &\geq \operatorname{vol}(K')/\operatorname{vol}(K' + B(1)) \\ &\geq \left(1 + \frac{2}{n}\right)^{-n}, \end{aligned}$$

We can therefore sample nearly uniformly from K in polynomial time, and we fully polynomial time approximation scheme as stated.

7. Modification of a theorem of Hoeffding

opulation C consist of n real values $c_1 \geq c_2 \geq \cdots \geq c_n \geq 0$. Let $c_{i_1}, c_{i_2}, \ldots, c_{i_t}$, $> \cdots > i_t$ denote a random sample drawn without replacement from C. Let $+ c_{i_2} + \cdots + c_{i_k}$ for $k = 1, 2, \ldots, t$. Let $\mu = \frac{1}{n}\sum_{i=1}^{n} c_i$. Hoeffding proved

7.1. *If $0 \leq c_i \leq \alpha$ for $i = 1, 2, \ldots, n$,*

$$\Pr(S_t - t\mu > x) \leq \exp\left\{-\frac{2x^2}{t\alpha^2}\right\} \qquad \textit{for all } x \geq 0.$$

not suitable for us, because we do not have enough control over the size of α. e the following theorem, which we believe is of interest in its own right.

7.2. *With the above notation*

$$(S_t - t\mu > S_m) = O(\exp\{-m^2(t-m)^2/t^3\}) \qquad \textit{for } t = m+1, \ldots, n.$$

et $T_j = c_1 + c_2 + \cdots + c_j$ for $j = 1, \ldots, n$ and $c = c_{i_m}$. If $S_t > t\mu + S_m$, then for be chosen later) either

$$S_m > (t-m)\frac{T_n - T_{i_m}}{n - i_m} + cx,$$

$$n)\frac{T_n - T_{i_m}}{n - i_m} + cx > t\mu.$$

ndle (i) by conditioning on $c_{i_1}, c_{i_2}, \ldots, c_{i_m}$ and applying Theorem 7.1. This yields

$$\Pr((\mathrm{i})) \leq e^{-2x^2/(t-m)}. \tag{22}$$

e (ii), we define δ by $n - i_m = \frac{n}{t}(t-m)(1-\delta)^{-1}$ and replace (ii) by the inequality $\frac{T_{i_m}t}{n}(1-\delta) > t\mu\delta$.

hat

$$T_{i_m}/i_m \geq \max\{\mu, c\}. \tag{23}$$

point we bound $|\delta|$ probabilistically. Now i_m is distributed as the mth largest a random t-set X chosen from $[n]$. Thus $\bar{i}_m = E(i_m) = nm/t$. Let $\theta = \bar{i}_m - i_m$ so $\theta/(n - \bar{i}_m + \theta)$ and $\theta = \delta n\left(1 - \frac{m}{t}\right)(1-\delta)^{-1}$. Now let $Z_k = |X \cap [k]|$. We observe ny $y > 0$,

$$\theta > y \;\Rightarrow\; Z_{\lfloor \bar{i}_m - y \rfloor} \geq m$$

and

$$\theta < -y \;\Rightarrow\; Z_{\lceil \bar{i}_m + y \rceil} \leq m.$$

But for any k, Z_k is distributed as the random variable S_t of Theorem 7.1, where C consists of k 1's and $n-k$ 0's. Thus $E(Z_k) = kt/n$, and applying the theorem gives

$$\Pr(|\theta| \geq y) \leq 2e^{-2y^2t/n^2}. \tag{24}$$

Case 1: $\delta < 0$. It follows from (23) that

$$\begin{aligned} (\mathrm{ii'}) \quad &\Rightarrow \quad \frac{T_{i_m}}{i_m}x - \frac{T_{i_m}t}{n}(1-\delta) \quad &\geq \quad t\frac{T_{i_m}}{i_m}\delta, \\ &\Rightarrow \quad x - \tfrac{i_m t}{n}(1-\delta) \quad &\geq \quad t\delta. \end{aligned}$$

Substituting $i_m = \frac{n(m-t\delta)}{t(1-\delta)}$, we obtain

$$(\mathrm{ii'}) \Rightarrow \; x \geq m.$$

We take $x = m/2$ from now on, so

$$\Pr((ii) \text{ and } \delta < 0) = 0. \tag{25}$$

Case 2: $\delta \geq 0$. Applying (23), we see now that (with $x = m/2$)

$$\begin{aligned} (\mathrm{ii'}) \quad &\Rightarrow \quad \frac{m}{2} - \frac{i_m}{n}t(1-\delta) \quad &\geq \quad 0 \\ &\Rightarrow \quad \frac{m}{2} - i_m\frac{t-m}{n-i_m} \quad &\geq \quad 0 \\ &\Rightarrow \quad i_m \quad &\leq \quad \frac{nm}{2t-m} \\ &\Rightarrow \quad \theta \quad &> \quad \frac{mn}{2t}\left(1 - \frac{m}{t}\right). \end{aligned}$$

Hence, from (24) we have

$$\Pr((\mathrm{ii}) \text{ and } \delta \geq 0) = O(\exp\{-m^2(t-m)^2/t^3\}). \tag{26}$$

The theorem follows from (22), (25) and (26). □

References

[1] Applegate, D. and Kannan, R. (1991) Sampling and integration of near log-concave functions. *Proc. 23rd ACM Symposium on Theory of Computing* 156–163.

[2] Broder, A. Z. (1986) How hard is it to marry at random? (On the approximation of the permanent.) *Proceedings of the 18th Annual ACM Symposium on Theory of Computing* 50–58. (Erratum in *Proceedings of the 20th Annual ACM Symposium on Theory of Computing* (1988) 551.)

[3] Dyer, M. E. and Frieze, A. M. (1991) Computing the volume of convex bodies: a case where randomness provably helps. In: Bollobás, B. (ed.) Probabilistic Combinatorics and its Applications. *AMS Proceedings of Symposia in Applied Mathematics* **44** 123–169.

] Dyer, M. E., Frieze, A. M. and Kannan, R. (1991) A random polynomial time algorithm for approximating the volume of convex bodies. *Journal of the Association for Computing Machinery* **38** 1–17.

] Hoeffding, W. (1963) Probability inequalities for sums of bounded random variables. *Journal of the American Statistical Association* **58** 13–30.

] Jerrum, M. R. and Sinclair, A. J. (1989) Approximating the permanent. *SIAM Journal on Computing* **18** 1149–1178.

] Jerrum, M. R. and Sinclair, A. J. (1989) Polynomial-time approximation algorithms for the Ising model, Department of Computer Science, Edinburgh University. (To appear in *SIAM Journal on Computing*.)

] Jerrum, M. R., Valiant, L. G. and Vazirani, V. V. (1986) Random generation of combinatorial structures from a uniform distribution. *Theoretical Computer Science* **43** 169–188.

] Jerrum, M. R. and Vazirani, U. (1992) A mildly exponential approximation algorithm for the permanent. *Proceedings of the 33rd Annual IEEE Symposium on Foundations of Computing* 320-326.

0] Karzanov, A. and Khachiyan, L. (1990) *On the conductance of order Markov chains*. Technical Report DCS TR 268, Rutgers University.

1] Lovász, L. (1979) *Combinatorial problems and exercises*, North-Holland, Amsterdam.

2] Lovász, L. and Simonovits, M. (1990) The mixing rate of Markov chains, an isoperimetric inequality and computing the volume. *Proceedings of the 31st Annual IEEE Symposium on Foundations of Computer Science* 346–354.

3] Lovász, L. and Simonovits, M. (1992) Random walks in a convex body and an improved volume algorithm. *Proceedings of the 33rd Annual IEEE Symposium on Foundations of Computer Science.*

4] Mihail, M. and Winkler, P. (1992) On the number of Euler orientations of a graph. *Proceedings of the 3rd Annual ACM-SIAM Symposium on Discrete Algorithms* 138–145.

5] Sinclair, A. J. and Jerrum, M. R. (1989) Approximate counting, uniform generation and rapidly mixing Markov chains. *Information and Computation* **82** 93–133.

Combinatorics, Probability and Computing (1993) 2, 285–299

Factorization in $F_q[x]$ and Brownian Motion

JENNIE C. HANSEN[†]

Actuarial Mathematics and Statistics Department, Heriot-Watt University, Edinburgh, Scotland

Received 14 September 1992; revised 2 July 1993

For Paul Erdős on his 80th birthday

We consider the set of polynomials of degree n over a finite field and put the uniform probability measure on this set. Any such polynomial factors uniquely into a product of its irreducible factors. To each polynomial we associate a step function on the interval [0,1] such that the size of each jump corresponds to the number of factors of a certain degree in the factorization of the random polynomial. We normalize these random functions and show that the resulting random process converges weakly to Brownian motion as $n \to \infty$. This result complements earlier work by the author on the order statistics of the degree sequence of the factors of a random polynomial.

1. Introduction

In this paper we study the factorization of random polynomials over the finite field F_q, q a prime power. Specifically, let Π_n denote the monic polynomials of degree n over F_q and let μ_n denote the uniform measure on Π_n. Any $f(x) \in \Pi_n$ factors uniquely, and the degrees of its factors determine a partition of the integer n. To investigate the limiting distribution of such partitions with respect to the measure μ_n as $n \to \infty$, we introduce the counting functions $\alpha_k : \bigcup_{n=1}^{\infty} \Pi_n \to \mathbb{Z}$ defined by setting $\alpha_k(f)$ equal to the number of factors in f of degree k. Now let $p(n) = |\Pi_n| = q^n$ and let $c(n)$ denote the number of irreducible monic polynomials of degree n. Then the joint distribution of $\alpha_1, \alpha_2, \ldots, \alpha_n$ with respect to μ_n can be expressed in terms of $p(n)$ and $c(1), c(2), \ldots, c(n)$ as follows:

$$\mu_n(\alpha_1 = m_1, \ldots, \alpha_n = m_n) = \frac{1}{p(n)} \prod_{k=1}^{n} \binom{m_k + c(k) - 1}{m_k}, \tag{1}$$

provided $\sum_{k=1}^{n} km_k = n$, ($\mu_n(\alpha_1 = m_1, \ldots, \alpha_n = m_n) = 0$ otherwise). We call the vector $(\alpha_1(f), \ldots, \alpha_n(f))$ the type vector of $f \in \Pi_n$.

[†] This research was partially supported by NSF grant DMS-90 099074.