論文審査の結果の要旨

氏　名　　原瀬　晋

論文題目:
Fast lattice reduction algorithms for optimizing $\mathbf{F}_2$-linear pseudorandom number generators
($\mathbf{F}_2$-線形擬似乱数発生法の最適化のための高速格子簡約アルゴリズム)

擬似乱数発生法とは、乱数のように見える数列を、決定性のアルゴリズムにより計算機内で高速かつ再現性のあるように生成する方法を指す。計算機による科学シミュレーションにおいて、確率的な要素を含む部分には擬似乱数は欠かせない。また、近年の計算機の並列化に伴い、各計算処理単位システムごとに相異なる擬似乱数発生器を配置することが多くなり、高速で高品質な擬似乱数発生法を、非常に多数用意する必要性が増えてきた。

擬似乱数発生法として現在最も有力なものは、二元体 $\mathbf{F}_2$ 上のベクトル空間を状態空間とし、線形な状態遷移関数と出力関数により状態を変移させつつ出力列を得る、$\mathbf{F}_2$ 線形擬似乱数発生法である。擬似乱数の品質を測る重要な評価基準としては、v ビット精度での高次元均等分布性が有力である。擬似乱数の出力列を [0,1] 実数列に正規化して k 個ずつの組にわけ、k 次元単位立方体内に擬似ランダムな点を一周期に渡って生成した際、各座標に関して v ビット精度で一様に点が分布しているとき、この擬似乱数列は v ビット精度で k 次元一様分布しているという。そのような k の最大値を $k(v)$ で表す。$k(v)$ が大きいほど擬似乱数の品質は良いと考えられるが、状態空間の次元 d に対して $k(v) \leq d/v$ なる上限がある。

生成する擬似乱数自体の精度を w ビットとする。$1 \leq v \leq w$ の各 v について $k(v)$ が上限に近いとき、擬似乱数は（作為的なものを除けば）通常の統計的検定に合格することが経験的に知られており、この基準に基づくパラメータ探索が有効である。しかし、d が大きいとき、$k(v)$ の計算には大きな時間がかかり、パラメータ検索におけるボトルネックとなっていた。本研究以前の最速アルゴリズムは次の通り：v ビット出力の無限列に対応するベクトル値の生成母関数を考えたとき、初期状態として全ての状態を動かして得られる母関数の集合が多項式係数格子を生成するが、その簡約基底のノルムの最大値が $k(v)$ を与える (Couture-Tezuka-L'Ecuyer, 1993)。それを、双対格子により計算する（Couture-L'Ecuyer, 2000）。

これに対し、本論文では、(1) 状態空間を用いて格子点を表現しメモリ使用量とビット演算数を減らす、(2)w 次元空間における簡約基底から、順番に $w-1$ 次元、$w-2$ 次元の簡約基底を計算することで、前計算を有効利用する、(3)Mulders-Strjohann(2003) による高速簡約基底計算を利用する、という三つの工夫により、$k(v)$ $(1 \leq v \leq w)$ の計算に要するビット演算の回数を $2wd^2 + \frac{1}{2}w^2d + \frac{1}{2}w^2(w+1)$ に減らすことに成功した。これは、前述の Couture-L'Ecuyer 双対格子法の約 $1/w$ である。実際、計算機実験により速度を測定し、$w = 32$, $d = 19937$ では 20 倍程度の高速化になることを確認している。このアルゴリズムは、$\mathbf{F}_2$ 線形擬似乱数発生法のパラメータを自動的に探索するソフトウェアである Dynamic Creator 及び MTGPDC に斎藤睦夫広島大学助教の手により組み込まれ、ホームページから配布されており、世界的に利用が進んでいる。この研究結果の一部は米国数学会出版の Mathematics of Computation に出版されており、残りは投稿中である。

以上によって、論文提出者　原瀬　晋は、博士（数理科学）の学位を受けるにふさわしい十分な資格があると認める。