

PHASE TRANSITION AND FINITE-SIZE SCALING
FOR THE INTEGER PARTITIONING PROBLEM

CHRISTIAN BORGS¹, JENNIFER CHAYES¹ AND BORIS PITTEL^{2,*}

¹*Microsoft Research, 1 Microsoft Way, Redmond, WA 98052*

²*Department of Mathematics, Ohio State University, Columbus, Ohio 43210*

August 2001

Dedicated to D. E. Knuth on the occasion of his 64th birthday.

Abstract. We consider the problem of partitioning n randomly chosen integers between 1 and 2^m into two subsets such that the discrepancy, the absolute value of the difference of their sums, is minimized. A partition is called *perfect* if the optimum discrepancy is 0 when the sum of all n integers in the original set is even, or 1 when the sum is odd. Parameterizing the random problem in terms of $\kappa = m/n$, we prove that the problem has a phase transition at $\kappa = 1$, in the sense that for $\kappa < 1$, there are many perfect partitions with probability tending to 1 as $n \rightarrow \infty$, while for $\kappa > 1$, there are no perfect partitions with probability tending to 1. Moreover, we show that this transition is first-order in the sense the derivative of the so-called entropy is discontinuous at $\kappa = 1$.

We also determine the finite-size scaling window about the transition point: $\kappa_n = 1 - (2n)^{-1} \log_2 n + \lambda_n/n$, by showing that the probability of a perfect partition tends to 1, 0, or some explicitly computable $p(\lambda) \in (0, 1)$, depending on whether λ_n tends to $-\infty$, ∞ , or $\lambda \in (-\infty, \infty)$, respectively. For $\lambda_n \rightarrow -\infty$ fast enough, we show that the number of perfect partitions is Gaussian in the limit. For $\lambda_n \rightarrow \infty$, we prove that with high probability the optimum partition is unique, and that the optimum discrepancy is $\Theta(2^{\lambda_n})$. Within the window, i.e., if $|\lambda_n|$ is bounded, we prove that the optimum discrepancy is bounded. Both for $\lambda_n \rightarrow \infty$ and within the window, we find the limiting distribution of the (scaled) discrepancy. Finally, both for the integer partitioning problem and for the continuous partitioning problem, we find the joint distribution of the k smallest discrepancies above the scaling window.

* Research of B. Pittel supported by Microsoft and by NSF grant # DMS-9803410.

1. Introduction.

This paper is dedicated, with great admiration, to Donald Knuth on the happy occasion of his 64th birthday. His work has been an inspiration to us throughout the years. We use this occasion to provide complete proofs and to give several extensions of the results first announced in [BCP].

There has recently been much interest in the study of phase transitions in random combinatorial problems. A combinatorial phase transition is an abrupt change in the qualitative behavior of the problem as an appropriately defined parameter is varied. The classic combinatorial phase transition occurs in the random graph model of Erdős and Rényi [ER1,ER2]. There one considers a graph on n vertices with edge occupation probability α/n . As the parameter α passes through 1, the model undergoes a phase transition in the sense that the size of the largest connected component changes from order $\log n$ to order n . More recently, there has been much study of the phase transition in the random k -SAT model, both by heuristic and rigorous methods; see [BCKW] and references therein. In k -SAT, the instances are formulas in conjunctive normal form; each formula has m clauses, and each clause has k distinct literals drawn uniformly at random from among n Boolean variables and their negations. For fixed $k \geq 2$, the model undergoes a sharp transition from solvability to insolvability as the parameter $\alpha = m/n$ passes through a particular k -dependent value [Fri].

In the language of mathematical physics, phase transitions occur only in the so-called thermodynamic limit, that is, in the limit of an infinite system. Finite-size scaling describes the approach of a finite system to the thermodynamic limit, in particular, the “broadening” of the transition point into a “scaling window” due to finite-size effects, and the behavior of the relevant functions in the scaling window. Finite-size scaling results are known for both the random graph model [Bol,Luc,JKLP] and the 2-SAT problem [BCKW]; in both cases, the width of the window is $n^{-1/3}$. But the question of finite-size scaling is open for k -SAT with $k \geq 3$.

The integer partitioning problem is a classic NP-complete problem of combinatorial optimization. In the version considered here, an instance is a given a set of n m -bit integers drawn uniformly at random from $[M] = \{1, 2, \dots, M\}$ with $M = 2^m$. The problem is to partition the given set into two subsets in order to minimize the absolute value of the difference between the sum of the integers in the two subsets, the so-called *discrepancy*. Clearly, the smallest possible discrepancy is 0 when the sum of all of the integers is even, and 1 when the sum is odd; a partition with this discrepancy is called *perfect*. In this work, we prove that the optimum partitioning problem undergoes a sharp transition as a function of the parameter $\kappa = m/n$, characterized by a dramatic change in the probability of a perfect partition. For m and n tending to infinity in the limiting ratio κ , the probability of a perfect partition tends to 1 for $\kappa < 1$, while the probability tends to 0 for $\kappa > 1$. Our result was inspired by the results of Mertens [Mer1] who gave an ingenious, nonrigorous argument for the existence of a phase transition in optimum partitioning.

We also derive the finite-size scaling of the system about the transition point $\kappa = 1$.

Namely, in terms of the more detailed parameterization $m = \kappa_n n$ with

$$\kappa_n = 1 - \frac{\log_2 n}{2n} + \frac{\lambda_n}{n}, \quad (1.1)$$

the probability of a perfect partition tends to 1, 0, or a computable λ -dependent constant strictly between 0 and 1, depending on whether λ_n tends to $-\infty$, ∞ , or $\lambda \in (-\infty, \infty)$, respectively. To our knowledge, this is the first rigorous analysis of finite-size scaling in an NP-complete problem. Equation (1.1) is the analogue of the scaling $\alpha_n = 1 + \lambda_n/n^{1/3}$ in the random graph problem [Bol,Luc,JKLP] and the 2-SAT problem [BCKW]. Here the scaling window is much smaller than it is in the random graph or 2-SAT, namely it is of width $\Theta(1/n)$ rather than $\Theta(1/n^{1/3})$. Also here, in contrast to the random graph and 2-SAT, the center of the scaling window is shifted from its limiting value by an amount which is larger than the width of the window itself, namely $(2n)^{-1} \log_2 n$ versus $\Theta(1/n)$.

Finally, we derive the limiting distributions of some of the fundamental quantities in the system. For $\lambda_n \rightarrow -\infty$, we get the distribution of the number of perfect partitions, which gives us the *entropy*. Both for $\lambda_n \rightarrow \infty$ and within the window, we get the detailed asymptotics of the distribution of the minimum discrepancy, which corresponds physically to the *ground state energy* of the system. We also get the joint distribution of the k smallest discrepancies, which corresponds physically to the *energy spectrum* of the system; we show that this spectrum is asymptotically well approximated by the spectrum of the so-called random energy model of Derrida [Der].

The random optimum partitioning problem has been studied previously by both rigorous and nonrigorous methods. A great deal of rigorous work has been done for the partitioning problem with random numbers drawn from a compact interval in \mathbb{R} , which we will henceforth refer to as the continuous case. This is conceptually analogous to the integer partitioning problem with $m \gg n$. Karmarkar and Karp [KK] gave a linear time algorithm for a suboptimal solution with a typical discrepancy of size $O(n^{-c \log^2 n})$ for some constant $c > 0$; see [Yak] for a proof of the KK-conjecture that the discrepancy obtained by their algorithm is indeed of the order $n^{-\theta(\log^2 n)}$.

The optimum solution was studied by Karmarkar, Karp, Lueker and Odlyzko [KKLO] who proved that the typical minimum discrepancy is much smaller, namely of order $O(2^{-n} \sqrt{n})$. More recently, Lueker [Lue] proved exponential bounds for the *expected* minimum discrepancy. Note that all of these results correspond to $m \gg n$, and hence $\kappa \rightarrow \infty$, well above the phase transition studied here.

There have also been (nonrigorous) studies of optimum partitioning in the theoretical physics and artificial intelligence communities, where the possibility of a phase transition was studied. Fu [Fu] studied the continuous case and noted that the minimum discrepancy is analogous to the ground state energy of an infinite-range, random antiferromagnetic spin model, but concluded incorrectly that the model did not have a phase transition. Gent and Walsh [GW] examined the problem numerically and introduced the parameter $\kappa = m/n$. They noticed that the number of perfect partitions falls off dramatically at a transition point estimated to be close to $\kappa = 0.96$. Ferreira and Fontanari studied the random spin model of Fu, and used statistical mechanical methods to get estimates of the optimum partition [FF1]

and to evaluate the average performance of simple heuristics [FF2]. Our work was motivated by the beautiful paper of Mertens [Mer1], who used statistical mechanical methods and the parameterization of Gent and Walsh to derive a compelling argument for a phase transition. In a later work, Mertens [Mer2] analyzed Fu's model by heuristically approximating it in terms of Derrida's random energy model [Der], and thereby obtained the limiting distribution of the k^{th} smallest discrepancy.

Merten's random energy model result [Mer2], albeit nonrigorous, suggested a substantial sharpening of the rigorous results of [KKLO] and [Lue]. Our analysis of the *integer* partitioning problem provides a rigorous justification of Merten's approximation both for the integer and the continuous partitioning problems, at least insofar as the joint distribution of the k (finite) smallest discrepancies is concerned. We thereby obtain essentially optimal results for the continuous problem studied originally by Karmarkar, Karp, Lueker and Odlyzko [KKLO], and the analogous results in the integer case.

It is worth noting that the optimum partitioning problem is closely related to several other classic problems of combinatorial optimization. The first is the "multi-way" partition problem in which a set of "weights" is to be partitioned into $N \geq 3$ subsets (parts), so that the sums of the weights in the N parts are as close to equal as possible. Graham [Gra] developed a linear-time $\frac{4}{3}$ -approximation algorithm for a version of this problem in which the goal is to minimize the weight of the heaviest part. The multi-way problem was also considered by [KKLO], who noted that their analysis of the minimum discrepancy would extend in a natural way to this case also. A second related problem is the so-called subset sum problem, in which one tries to find subsets of a given set of integers which sum to (or near to) a prescribed target number. This problem reduces to a study of solutions of linear equations of the form $\sum_i s_i X_i = T$, where X_i are the numbers in the given set, $s_i \in \{0, 1\}$ represents whether or not X_i is included in a particular subset, and T is the target number. A key idea is to express the total number of solutions to these equations via a Fourier-type inversion integral, a paradigm championed by Freiman [Fre]; see also Alon and Freiman [AF], Chaimovich and Freiman [CF]. We will use an analogous integral representation in our study of the integer partitioning problem. Some of the methods and results presented here can be used to obtain stronger results for the subset sum problem, but we will not pursue this here.

2. Statement of Results.

Let us begin with a little notation. The instances of the problem are sets of n integers X_1, \dots, X_n chosen independently and uniformly from $[M] = \{1, 2, \dots, M\}$, where M is an integer $M \geq 2$. For notational convenience, we will often write M as $M = 2^m$, even when $m = \log_2 M$ is not an integer. We will generally fix m to be some function of n (e.g., by taking $m = \kappa n$). The probability measure induced by the random variables $\mathbf{X} = \{X_1, \dots, X_n\}$ will be denoted by \mathbb{P}_n , and expectation by \mathbb{E}_n . When no confusion arises, we will drop the subscript n . The event that " $\sum_{j=1}^n X_j$ is even" will be denoted by \mathcal{E}_n , while the event that the sum is odd will be denoted by \mathcal{O}_n . As usual we will say that an event happens with high probability (w.h.p.) if the probability that it happens goes to one as $n \rightarrow \infty$. Finally, X will denote a generic random variable distributed uniformly on $[M]$.

There are 2^n ways to form an *ordered* partition of n integers X_1, \dots, X_n into two sets.

Each such partition can be labelled by $\boldsymbol{\sigma} = (\sigma_1, \dots, \sigma_n)$ with $\sigma_j \in \{-1, 1\}$, so that, say, the first set is $\{X_j : \sigma_j = -1\}$, and the second is $\{X_j : \sigma_j = 1\}$. The discrepancy of the partition with label $\boldsymbol{\sigma}$ is $|\boldsymbol{\sigma} \cdot \mathbf{X}| = |\sum_{j=1}^n \sigma_j X_j|$. Let d_n denote the optimum (minimum) discrepancy of \mathbf{X} over all $\boldsymbol{\sigma}$:

$$d_n = d_n(\mathbf{X}) = \min_{\boldsymbol{\sigma}} |\boldsymbol{\sigma} \cdot \mathbf{X}|. \quad (2.1)$$

Clearly d_n is even on \mathcal{E}_n , and odd on \mathcal{O}_n . A partition with $|\boldsymbol{\sigma} \cdot \mathbf{X}| \leq 1$ (i.e., $|\boldsymbol{\sigma} \cdot \mathbf{X}| = 0$ on \mathcal{E}_n and $|\boldsymbol{\sigma} \cdot \mathbf{X}| = 1$ on \mathcal{O}_n) is called *perfect*, and a partition with $|\boldsymbol{\sigma} \cdot \mathbf{X}| = d_n$ is called an optimum or minimum partition. Let $Z_n = Z_n(\mathbf{X})$ and $\tilde{Z}_n = \tilde{Z}_n(\mathbf{X})$ denote the number of perfect and optimum partitions of \mathbf{X} , respectively. Of course, $Z_n = \tilde{Z}_n$ iff $d_n = 0$ or $d_n = 1$. Note that a partition with label $\boldsymbol{\sigma}$ has the same discrepancy as that with label $-\boldsymbol{\sigma}$. The random variables $Z_n(\mathbf{X})$ and $\tilde{Z}_n(\mathbf{X})$ therefore take values in the even non-negative integers.

Our first result shows that the model has a sharp phase transition at $\kappa = 1$.

Theorem A. *Let $m = \kappa_n n$, and assume that there exists $\lim_{n \rightarrow \infty} \kappa_n = \kappa \in [0, \infty]$. Then*

$$\lim_{n \rightarrow \infty} \mathbb{P}_n(\exists \text{ a perfect partition}) = \begin{cases} 1 & \text{if } \kappa < 1 \\ 0 & \text{if } \kappa > 1. \end{cases} \quad (2.2)$$

Our next result uses the more sensitive parameterization (1.1) to strengthen Theorem A, and, in particular, to establish the existence of a scaling window.

Theorem B. *Let $m = \kappa_n n$, with κ_n as in (1.1), and assume that $\lim_{n \rightarrow \infty} \lambda_n = \lambda$ exists. Then*

$$\lim_{n \rightarrow \infty} \mathbb{P}_n(\exists \text{ a perfect partition}) = \begin{cases} 1 & \text{if } \lambda = -\infty \\ 1 - \frac{1}{2} r(\lambda)(r(\lambda) + 1) & \text{if } \lambda \in (-\infty, \infty) \\ 0 & \text{if } \lambda = \infty, \end{cases} \quad (2.3)$$

where $r(\lambda) = \exp\left(-\sqrt{\frac{3}{2\pi}} 2^{-\lambda}\right)$.

Our next result gives detailed information on the distribution of the number of perfect and optimum partitions, Z_n and \tilde{Z}_n , and therefore also on the *entropy*, defined as

$$S_n = \log_2 \tilde{Z}_n. \quad (2.4)$$

Note that, since $\tilde{Z}_n \geq 1$, S_n is well-defined and non-negative for all \mathbf{X} , as a ‘‘physical’’ entropy should be. Note that $\log_2 Z_n$ would not be a well-defined entropy since Z_n can vanish; an ‘‘entropy’’ so defined could lead to statements incompatible with the principles of statistical mechanics, see e.g. [Mer1].

Theorem C. *Let $m = \kappa_n n$, with κ_n as in (1.1), and define*

$$c_M = \mathbb{E}\left(\frac{X^2}{M^2}\right) = \frac{1}{3} + \frac{1}{2M} + \frac{1}{6M^2}. \quad (2.5)$$

i) If $\lambda_n \rightarrow -\infty$, then

$$\left(\frac{2^{1+|\lambda_n|}}{\sqrt{2\pi c_M}}\right)^{-1} Z_n \rightarrow \begin{cases} 1 & \text{on } \mathcal{E}_n \\ 2 & \text{on } \mathcal{O}_n \end{cases} \quad (2.6)$$

in probability and in mean,

$$S_n - |\lambda_n| + \frac{1}{2} \log_2 c_M \rightarrow \begin{cases} \frac{1}{2} \log_2(2/\pi) & \text{on } \mathcal{E}_n \\ \frac{1}{2} \log_2(8/\pi) & \text{on } \mathcal{O}_n \end{cases} \quad (2.7)$$

in probability, and

$$n^{-1}(S_n - |\lambda_n|) \rightarrow 0 \quad (2.8)$$

in mean.

ii) If $\lambda_n \rightarrow \lambda \in (-\infty, \infty)$, then S_n is bounded in probability, so that in particular

$$n^{-1}S_n \rightarrow 0 \quad (2.9)$$

in probability. More precisely, on the event \mathcal{O}_n the entropy S_n converges (in distribution) to $1 + \log_2 P(\mu)$ where $P(\mu)$ is Poisson with parameter $\mu = 2^{-\lambda} \sqrt{6/\pi}$ conditioned on $\{P(\mu) \geq 1\}$; on the event \mathcal{E}_n the entropy S_n converges to $1 + \log_2 Q(\mu)$, where $Q(\mu) = P(\mu/2)$ with probability $1 - e^{-\mu/2}$ and $Q(\mu) = P(\mu)$ with probability $e^{-\mu/2}$.

iii) If $\lambda_n \rightarrow \infty$, then with probability tending to 1, the optimum partition is unique up to the symmetry $\sigma \rightarrow -\sigma$. In particular, $\mathbb{P}(S_n = 1) \rightarrow 1$ as $n \rightarrow \infty$.

Corollary. Assume that m/n converges to some $\kappa < \infty$. Then the entropy per variable, $s_n = n^{-1}S_n$, converges in probability to (the deterministic function)

$$s(\kappa) = \max\{0, 1 - \kappa\}, \quad (2.10)$$

so that, in particular, the limiting entropy per variable does not have a continuous derivative at $\kappa = 1$.

Remarks.

- i) The reader will note that the statements below the window in Theorems A and B are immediate corollaries of Theorem C(i), equation (2.6), which strengthens the statement $Z_n > 0$ w.h.p. by giving a law of large numbers for Z_n .
- ii) If the condition of Theorem C(i) is slightly strengthened to $\lambda_n + \log_2 n \rightarrow -\infty$, we can prove even more, namely a central limit theorem stating that, in the limit, Z_n has a Gaussian distribution with mean implicit in (2.6), and standard deviation roughly equal to the mean times $n^{-1/2}$. See Theorem 4.1 in Section 4. This allows us to show that S_n is also Gaussian in the limit and to replace (2.7) by the following stronger result: given $\varepsilon > 0$, in probability,

$$\begin{aligned} \lim_{n \rightarrow \infty} \frac{S_n - |\lambda_n| + \frac{1}{2} \log_2(\pi c_M/2)}{n^{-(1/2)+\varepsilon}} &= 0, & \text{on } \mathcal{E}_n, \\ \lim_{n \rightarrow \infty} \frac{S_n - |\lambda_n| + \frac{1}{2} \log_2(\pi c_M/8)}{n^{-(1/2)+\varepsilon}} &= 0, & \text{on } \mathcal{O}_n, \end{aligned} \quad (2.11)$$

see Theorem 4.2 .

- iii) In statistical physics, phase transitions are characterized by non-analyticities in derivatives of thermodynamic potentials. These non-analyticities may be discontinuities or smoother non-analyticities. First-order phase transitions are characterized by a discontinuity in a first derivative of a thermodynamic potential (but not necessarily in all first derivatives of all thermodynamic potentials). By contrast, all first derivatives of thermodynamic potentials are continuous at second-order phase transitions; the corresponding second derivatives usually diverge. In the optimum partitioning problem, the entropy—which is a first derivative of a thermodynamic potential—is continuous, but its derivative is discontinuous. This is analogous to the behavior of the entropy of the Ising model in a magnetic field, which has a first-order phase transition as the magnetic field passes through zero.

Another characteristic which can be used to distinguish first- and second-order phase transitions is the width of the scaling window. In a first-order phase transition, such as the Ising model in a field, the scaling window of a system of size n is of width n^{-1} ; see [BK]. By contrast, second-order phase transitions have scaling windows of width n^{-b} for some $b < 1$, as has been established for the random graph [Bol,Luc] and the 2-SAT problem [BBCKW]. In the optimum partitioning problem, the scaling window of is width n^{-1} . Hence we conclude that this problem has a first-order phase transition at $\kappa = 1$.

Our next theorem gives detailed distributional estimates of the discrepancy d_n defined in (2.1). Noting that $|\sigma \cdot \mathbf{X}|$ may be viewed as the energy of the “configuration” σ in the random instance \mathbf{X} , we see that the discrepancy can be identified with the *ground state energy* of instance \mathbf{X} . Above the window, the next theorem also gives the joint distribution of the k smallest discrepancies, and hence the energy spectrum of the problem. To make this precise, let D be the ordered multiset

$$D = \{d_{n,1} \leq d_{n,2} \leq \cdots \leq d_{n,2^n-1}\}$$

of all 2^{n-1} discrepancies.

Theorem D. *Let $m = \kappa_n n$, with κ_n as in (1.1).*

i) *If $\lambda_n \rightarrow -\infty$, then*

$$d_n \rightarrow \begin{cases} 0 & \text{in probability on } \mathcal{E}_n \\ 1 & \text{in probability on } \mathcal{O}_n. \end{cases} \quad (2.12)$$

ii) *If $\lim_{n \rightarrow \infty} \lambda_n \in (-\infty, \infty)$, then d_n is bounded in probability. More precisely, in the limit, d_n has a (modified) geometric distribution: for $\ell \geq 1$,*

$$\lim_{n \rightarrow \infty} \mathbb{P}_n \{d_n \geq \ell\} = \frac{1+r}{2} r^{\ell-1}, \quad (2.13)$$

with $r = r(\lambda)$ as defined in Theorem B.

iii) *If $\lambda_n \rightarrow \infty$, then $d_n/2^{\lambda_n}$ and its inverse are bounded in probability. In the limit, $d_n/2^{\lambda_n}$ has the following exponential distribution: for $a > 0$,*

$$\lim_{n \rightarrow \infty} \mathbb{P}_n \left(\frac{d_n}{2^{\lambda_n}} > a \right) = \exp \left(-\sqrt{\frac{3}{2\pi}} a \right). \quad (2.14)$$

More generally, let $d_{n,r}$ be the r^{th} smallest discrepancy. Then, for a fixed $\ell \geq 1$, the ℓ -tuple $2^{-(\lambda_n+1)}(d_{n,1}, \dots, d_{n,\ell})$ converges in distribution to $(W_1, W_1 + W_2, \dots, W_1 + \dots + W_\ell)$, where W_i are i.i.d. random variables, each distributed exponentially with parameter $(6/\pi)^{1/2}$.

Remark.

iv) Theorem D(iii) is a discrete counterpart of Stephan Mertens's (nonrigorous) result [Mer2] for partitions of random numbers which are uniformly distributed on $[0, 1]$. His statistical physics approach was based a heuristic mapping of this continuous problem into the so-called random energy model of Derrida [Der]. For the integer partitions, Mertens's analysis would require that the discrepancies of all 2^{n-1} distinct partitions can be approximated by the family of 2^{n-1} independent random variables, which individually have the same common distribution as the actual discrepancies. Theorem D(iii) shows that this approximation is indeed valid, insofar as the joint distribution of the (finite) k smallest discrepancies is concerned. In fact, Theorem D(iii) immediately implies the results of Mertens for the uniform distribution on $[0, 1]$, and optimally extends the rigorous results of [KKLO] and [Lue]. This is formulated in the next Theorem, which is proved in Section 6. We thank the referee for pointing out that this result follows easily from our other results and a coupling argument.

Theorem E. Consider the optimum partitioning problem for n random variables U_1, \dots, U_n chosen independently and uniformly at random from the interval $[0, 1]$. Let $\tilde{d}_{n,r}$ be the r^{th} smallest discrepancy of this continuous problem. Then, for any fixed $\ell \geq 1$, the ℓ -tuple $(2^{n-1}/\sqrt{n})(\tilde{d}_{n,1}, \dots, \tilde{d}_{n,\ell})$ converges in distribution to $(W_1, W_1 + W_2, \dots, W_1 + \dots + W_\ell)$, where W_i are i.i.d. random variables, each distributed exponentially with parameter $(6/\pi)^{1/2}$.

The scheme of our proof is as follows. The reader will notice that Theorem B is a corollary of Theorem D, and that Theorem D(i) follows from Theorem C(i), equation (2.6), while Theorem C(iii) follows from Theorem D(iii). The proof of Theorems A–D is therefore reduced to that of Theorem C (i)–(ii) and Theorem D(ii)–(iii). This is accomplished by detailed calculations using an integral representation to be described in Section 3. Also in Section 3, we formulate and prove estimates on the first and second moments of the number of partitions with a given discrepancy. These moment estimates allow us to establish Theorem C(i), as well as some statements in probability on S_n and d_n , namely the “in probability” statements of Theorems C(ii) and D(ii) and part of those in Theorem D(iii), see Proposition 3.2 in Section 3. In Section 4, for $\lambda_n + \log_2 \lambda_n \rightarrow \infty$, we formulate and prove distributional statements on our integral representations which allow us to establish Remark (ii) above. Section 5 is devoted to probabilistic bounds on the minimal discrepancy d_n , containing in particular the corresponding statements in Theorem D(iii) and D(ii), see Theorem 5.1, Theorem 5.2 and Corollary 5.3. The distribution of d_n above the window is then studied in Section 6, where we prove in particular Theorem D(iii). The distribution of d_n inside the window is studied in Section 7, where we prove Theorem D(ii) and C(ii).

3. The Integral Representation and Moment Estimates.

Recalling $M = 2^m$, we begin by rewriting (1.1) in the form:

$$2^{\lambda_n} = \frac{M\sqrt{n}}{2^n}. \quad (3.1)$$

Our proofs are based on an integral representation of $Z_{n,\ell}$, the number of partition with discrepancy ℓ . To derive this representation, we first write $Z_{n,\ell}$ as

$$Z_{n,\ell} = \sum_{\boldsymbol{\sigma}} \mathbb{I}(|\boldsymbol{\sigma} \cdot \mathbf{X}| = \ell), \quad (3.2)$$

where we use $\mathbb{I}(A)$ to denote the indicator of an event A , and then use the identity

$$\mathbb{I}(\boldsymbol{\sigma} \cdot \mathbf{X} = \ell) = \frac{1}{2\pi} \int_{-\pi}^{\pi} e^{i(\boldsymbol{\sigma} \cdot \mathbf{X} - \ell)x} dx \quad (3.3)$$

to sum over all 2^n configurations $\boldsymbol{\sigma}$. This gives the representation

$$Z_{n,\ell} = 2^n I_{n,\ell} \times \begin{cases} 1 & \text{if } \ell = 0 \\ 2 & \text{if } \ell > 0, \end{cases} \quad (3.4)$$

where $I_{n,\ell} = I_{n,\ell}(\mathbf{X})$ is the random integral

$$I_{n,\ell} = \frac{1}{2\pi} \int_{-\pi}^{\pi} \cos(\ell x) \prod_{j=1}^n \cos(xX_j) dx. \quad (3.5)$$

The first set of results, namely Theorem A, Theorem B outside the window, and Theorem C(i), follow from estimates on the first and second moments of $I_{n,\ell}$. Below we will state and prove these estimates. We then show how the estimates imply the theorems mentioned above. The central limit theorem, referred to in Remark (ii) following Theorem C, is a consequence of detailed estimates on the *random* integral $I_{n,\ell}$, rather than just on a few of its moments. The reader is referred to Section 4 for details.

Proposition 3.1. *Let $C_0 > 0$ be a finite constant, let $M = M(n)$ be an arbitrary function of n , let*

$$\gamma_n = \frac{1}{M\sqrt{2\pi n c_M}} \quad (3.6)$$

with c_M as in (2.5), and let ℓ and ℓ' be integers with $|\ell|/M \leq C_0$ and $|\ell'|/M \leq C_0$. Then

$$\mathbb{E}[I_{n,\ell}] = \gamma_n(1 + O(n^{-1})). \quad (3.7)$$

Furthermore

$$\mathbb{E}[I_{n,\ell}I_{n,\ell'}] = 2\gamma_n^2 \left(1 + O(n^{-1}) + O\left(\frac{n^{-1}}{\gamma_n 2^n}\right) \right) + \frac{\gamma_n}{2^n} (\delta_{\ell+\ell',0} + \delta_{\ell-\ell',0}) \quad (3.8)$$

if ℓ and ℓ' are of the same parity, i.e. both even or both odd, while $\mathbb{E}[I_{n,\ell}I_{n,\ell'}] = 0$ if ℓ and ℓ' are of different parity. In (3.7) and (3.8), the bounds implicit in the O -symbols are uniform in M and n , but depend on the constant C_0 .

Proof. We first use (3.5), independence of the X_j , and the Fubini theorem to get

$$\mathbb{E}[I_{n,\ell}] = \frac{1}{2\pi} \int_{-\pi}^{\pi} \cos(\ell x) f^n(x) dx \quad (3.9)$$

and

$$\mathbb{E}[I_{n,\ell}I_{n,\ell'}] = \frac{1}{(2\pi)^2} \iint_{x_1, x_2 \in (-\pi, \pi]} \cos(x_1 \ell) \cos(x_2 \ell') f^n(x_1, x_2) dx_1 dx_2 \quad (3.10)$$

where

$$f(x) := \mathbb{E}[\cos(xX)] = M^{-1} \sum_{j=1}^M \cos(jx) = M^{-1} \left[\frac{\sin((M+1/2)x)}{2 \sin(x/2)} - \frac{1}{2} \right], \quad (3.11)$$

$$f(x_1, x_2) := \mathbb{E}[\cos(x_1 X) \cos(x_2 X)] = \frac{1}{2} (f(x_1 + x_2) + f(x_1 - x_2)) \quad (3.12)$$

and $f^n(x)$ stands for $[f(x)]^n$.

In our analysis of the asymptotics of these integrals, we show that the major contributions come from values of the integration variables near the maxima of $|f(x)|$ and $|f(x_1, x_2)|$. Note, however, that the function f depends on the parameter M , which can grow as $n \rightarrow \infty$. Fortunately, a careful treatment of error terms will allow us to apply a variation of the standard saddle point method to get the desired asymptotics. When M is bounded, the proof of Proposition 3.1 is a straightforward application of the standard saddle-point methods, which we leave to the reader. The arguments below establish Proposition 3.1 for M larger than some M_0 , to be determined in the course of the proof.

Pick $1 < a < b$. If $x \in [-\pi, \pi]$ is such that $|2 \sin(x/2)| \geq b/M$, then

$$|f(x)| \leq \frac{1}{b} + \frac{1}{2M} \leq \frac{1}{a} \quad (3.13)$$

for M large enough. We will also use

$$|f(x)| \leq \frac{1}{M |\sin(x/2)|} \leq \frac{C}{M|x|}, \quad (3.14)$$

uniformly for $|x| \in (0, \pi]$, a direct consequence of (3.11). Here and below, C, C_1, C' , etc., stand for absolute positive constants. (In (3.14), C can be chosen as $\pi/2$.)

Notice that $x \in (-\pi, \pi)$ satisfies $|2 \sin(x/2)| \leq b/M$ iff $|x| \leq b_0/M$, where $b_0 = b_0(M)$ is defined for M large enough by the condition $2 \sin(b_0/(2M)) = b/M$ with $b_0/(2M) \in (0, \pi/2)$. Clearly $b_0(M) \rightarrow b$ as $M \rightarrow \infty$. By (3.13),

$$|f(x)| \leq \frac{1}{a} \quad \text{if } |x| \geq b_0/M.$$

Consider now $|x| \leq b_0/M$, and set $x = y/M$, i.e., $|y| \leq b_0$. Then, for $y \neq 0$,

$$f(x) = M^{-1} \left[\frac{\sin(y + y/(2M))}{2 \sin(y/(2M))} - \frac{1}{2} \right] = \frac{\sin y}{2M \tan(y/(2M))} + \frac{\cos y - 1}{2M},$$

and, since $\tan z > z$ on $(0, \pi/2)$,

$$|f(x)| \leq \left| \frac{\sin y}{y} \right| + \frac{1 - \cos y}{2M}.$$

Hence there exist a small enough constant $C_1 = C_1(b_0) > 0$ such that for M large enough

$$|f(x)| \leq e^{-C_1 y^2} \quad \text{if } |y| \leq b_0. \quad (3.15)$$

For $|y|$ sufficiently small, we also have

$$\begin{aligned} f(x) &= \mathbb{E}(\cos(y(X/M))) = \mathbb{E} \left(1 - \frac{y^2}{2} \cdot \frac{X^2}{M^2} + O(y^4) \right) \\ &= 1 - \frac{c_M}{2} y^2 + O(y^4) = \exp \left(-\frac{c_M}{2} y^2 + O(y^4) \right), \end{aligned} \quad (3.16)$$

with c_M as in (2.5), so that

$$f^n(x) = \exp \left(-n \frac{c_M}{2} y^2 \right) (1 + O(ny^4)). \quad (3.17)$$

Combining (3.17) and (3.15), we get

$$\begin{aligned} \frac{1}{2\pi} \int_{|x| \leq b_0/M} f^n(x) dx &= \frac{1}{2\pi M} \int_{|y| \leq n^{-1/2} \log n} \exp \left(-\frac{nc_M}{2} y^2 \right) dy \\ &\quad + O \left(M^{-1} \int_{|y| \leq n^{-1/2} \log n} ny^4 \exp \left(-\frac{nc_M}{2} y^2 \right) dy \right) \\ &\quad + O \left(M^{-1} \int_{|y| \geq n^{-1/2} \log n} e^{-nC_1 y^2} dy \right) \\ &= \frac{1}{M\sqrt{2\pi nc_M}} \left(1 + O(n^{-1}) + O(e^{-C' \log^2 n}) \right) \\ &= \frac{1}{M\sqrt{2\pi nc_M}} (1 + O(n^{-1})). \end{aligned} \quad (3.18)$$

and more generally

$$\begin{aligned}
\frac{1}{2\pi} \int_{|x| \leq b_0/M} \cos(\ell x) f^n(x) dx &= \frac{1}{2\pi M} \int_{|y| \leq n^{-1/2} \log n} \cos(\ell M^{-1} y) \exp\left(-\frac{nc_M}{2} y^2\right) dy \\
&+ O\left(\frac{1}{M\sqrt{2\pi nc_M}} \left(O(n^{-1}) + O(e^{-C' \log^2 n})\right)\right) \\
&= \frac{1}{M\sqrt{2\pi nc_M}} \left(\exp\left(-\frac{\ell^2}{2nM^2 c_M}\right) + O(n^{-1})\right).
\end{aligned} \tag{3.19}$$

Besides, by (3.13) and the definition of b_0 ,

$$\begin{aligned}
\int_{|x| \in [b_0/M, \pi]} |f(x)|^n dx &\leq \int_{|x| \in [b_0/M, \pi]} \left[\min\left\{a^{-1}, \frac{C}{Mx}\right\}\right]^n dx \\
&\leq \frac{2Ca}{M} a^{-n} + \int_{|x| \geq Ca/M} \left(\frac{C}{Mx}\right)^n dx \leq \frac{4Ca}{M} a^{-n} = O(a^{-n} M^{-1}).
\end{aligned}$$

Thus, for all integers ℓ and all $a > 1$,

$$\begin{aligned}
\mathbb{E}I_{n,\ell}(\mathbf{X}) &= \frac{1}{M\sqrt{2\pi nc_M}} \left(\exp\left(-\frac{\ell^2}{2nM^2 c_M}\right) + O(n^{-1})\right) + O(a^{-n} M^{-1}) \\
&= \gamma_n \left(\exp\left(-\frac{\ell^2}{2nM^2 c_M}\right) + O(n^{-1})\right),
\end{aligned} \tag{3.20}$$

where the constant implicit in $O(n^{-1})$ (and similar error terms below) depends on a . Under the assumption $\ell = O(M)$, this proves the estimate (3.7) for all sufficiently large M .

Next we turn to the second moment (3.10). Since $f(x_1, x_2) = f(\pm x_1, \pm x_2)$ we have

$$\begin{aligned}
\mathbb{E}[I_{n,\ell} I_{n,\ell'}] &= \left(\frac{1}{2\pi}\right)^2 \iint_{x_1, x_2 \in (-\pi, \pi]} e^{i(\ell x_1 + \ell' x_2)} f^n(x_1, x_2) dx_1 dx_2, \\
&= \left(\frac{1}{2\pi}\right)^2 \iint_{x_1, x_2 \in (-\pi, \pi]} e^{i\ell_1(x_1 + x_2)} e^{i\ell_2(x_1 - x_2)} f^n(x_1, x_2) dx_1 dx_2,
\end{aligned} \tag{3.21}$$

where

$$\ell_1 = (\ell + \ell')/2 \quad \text{and} \quad \ell_2 = (\ell - \ell')/2. \tag{3.22}$$

Let us consider a square Q with corners at $(0, \pm\pi), (\pm\pi, 0)$, so that $Q = \{(x_1, x_2) : |x_1| + |x_2| \leq \pi\}$. The coordinate axes partition Q into the four direct (isosceles) triangles. The integration square $[-\pi, \pi]^2$ consists of Q and four other direct triangles. Let us look at one of the latter triangles, in the positive quadrant say. It has its corners at $(0, \pi), (\pi, 0), (\pi, \pi)$.

Clearly, this triangle can be obtained via a parallel translation from the triangle with corners at $(-\pi, 0)$, $(0, -\pi)$, $(0, 0)$ in the direction determined by the vector $(1, 1)$. In this translation, every point (x_1, x_2) moves to a point (x'_1, x'_2) such that

$$x'_1 + x'_2 = x_1 + x_2 + 2\pi, \quad x'_1 - x'_2 = x_1 - x_2;$$

Since $f(x)$ is 2π -periodic, it follows from (3.12) that $f(x'_1, x'_2) = f(x_1, x_2)$. If $\ell + \ell'$ is even, then the other two factors in the integral (3.21) are invariant as well, and the contributions of the two triangles to the value of $\mathbb{E}[I_{n,\ell}I_{n,\ell'}]$ are equal to each other, while they cancel each other if $\ell + \ell'$ is odd, since in this case $e^{i\ell_1(x_1+x_2)} = -e^{i\ell_1(x'_1+x'_2)}$. The contributions from the other triangles in $[-\pi, \pi]^2 \setminus Q$ behave in a similar way, so that $\mathbb{E}[I_{n,\ell}I_{n,\ell'}]$ is twice the value of the integral over the square Q if $\ell + \ell'$ is even, and zero if $\ell + \ell'$ is odd. Changing to the integration variables $\xi_1 = x_1 + x_2$ and $\xi_2 = x_1 - x_2$, and observing that the Jacobian is $\partial(x_1, x_2)/\partial(\xi_1, \xi_2) = 1/2$, we therefore obtain that, for $\ell + \ell'$ even,

$$\mathbb{E}[I_{n,\ell}I_{n,\ell'}] = \frac{1}{(2\pi)^2} \iint_{\xi_1, \xi_2 \in (-\pi, \pi]} e^{i\ell_1\xi_1} e^{i\ell_2\xi_2} \phi^n(\xi_1, \xi_2) d\xi_1 d\xi_2, \quad (3.23)$$

where

$$\phi(\xi_1, \xi_2) = \frac{1}{2}(f(\xi_1) + f(\xi_2)). \quad (3.24)$$

Before analyzing the integral (3.23) in the general, we first consider the easier case $\ell = \ell' = 0$, i.e. we consider the integral

$$\mathbb{E}[I_{n,0}^2] = \frac{1}{(2\pi)^2} \iint_{\xi_1, \xi_2 \in (-\pi, \pi]} \phi^n(\xi_1, \xi_2) d\xi_1 d\xi_2. \quad (3.25)$$

As in the computation of $\mathbb{E}I_{n,0}(\mathbf{X})$, we clearly need to treat the points (x_1, x_2) according to how small $|\sin(\xi_1/2)|$ and $|\sin(\xi_2/2)|$ are. Consider first all $(\xi_1, \xi_2) \in (-\pi, \pi]^2$ such that

$$|2 \sin(\xi_1/2)| \leq b/M \quad \text{and} \quad |2 \sin(\xi_2/2)| \leq b/M.$$

Since $|\xi_1|, |\xi_2| \leq \pi$, the corresponding set of points (x_1, x_2) is a small neighborhood U_{b_0} of the origin $(0, 0)$ given by

$$U_{b_0} = \{(\xi_1, \xi_2) : |\xi_1| \leq b_0/M, |\xi_2| \leq b_0/M\}.$$

(Recall the definition of b_0 from the computation of $\mathbb{E}I_{n,0}(X)$.) For the points $(\xi_1, \xi_2) \in U_{b_0}$ we set $\xi_1 = \eta_1/M$ and $\xi_2 = \eta_2/M$ (so that $\max\{|\eta_1|, |\eta_2|\} \leq b_0$ whenever $(\xi_1, \xi_2) \in U_{b_0}$). As in (3.16), we have

$$\begin{aligned} \phi(\xi_1, \xi_2) &= \mathbb{E} \left[\frac{\cos(\eta_1(X/M)) + \cos(\eta_2(X/M))}{2} \right] \\ &= \mathbb{E} \left[1 - \frac{X^2(\eta_1^2 + \eta_2^2)}{4M^2} + O(\eta_1^4 + \eta_2^4) \right] \\ &= 1 - \frac{c_M(\eta_1^2 + \eta_2^2)}{4} + O(\eta_1^4 + \eta_2^4). \end{aligned}$$

Hence there exists a small enough $y^* \leq b_0/2$ such that in a *subneighborhood* $\max\{|\eta_1|, |\eta_2|\} \leq y^*$ of U_{b_0}

$$\phi(\xi_1, \xi_2) = \prod_{i=1}^2 \exp\left(-\frac{c_M \eta_i^2}{4} + O(\eta_i^4)\right).$$

Using (3.24), (3.15), and a little algebra, one can also show that there exist $C^* > 0$ such that in the whole neighborhood U_{b_0}

$$|\phi(\xi_1, \xi_2)| \leq \exp(-C^*(\eta_1^2 + \eta_2^2)).$$

So, as in (3.18), we get

$$\frac{1}{(2\pi)^2} \iint_{(\xi_1, \xi_2) \in U_{b_0}} \phi^n(\xi_1, \xi_2) d\xi_1 d\xi_2 = 2 \left(\frac{1}{M\sqrt{2\pi n c_M}} \right)^2 \cdot (1 + O(n^{-1})). \quad (3.26)$$

Therefore, the contribution of U_{b_0} to $\mathbb{E}[I_{n,0}^2(\mathbf{X})]$ is

$$2 \left(\frac{1}{M\sqrt{2\pi n c_M}} \right)^2 \cdot (1 + O(n^{-1})) = 2\gamma_n^2(1 + O(n^{-1})). \quad (3.27)$$

Consider the opposite case when both $|2 \sin(\xi_1/2)| \geq b_0/M$ and $|2 \sin(\xi_2/2)| \geq b_0/M$. Denote the corresponding subset of $(-\pi, \pi]^2$ by R . According to (3.13) and (3.14), for $(\xi_1, \xi_2) \in R$,

$$|\phi(\xi_1, \xi_2)| \leq \frac{1}{2}(\psi(\xi_1) + \psi(\xi_2));$$

$$\psi(z) := \min \left\{ a^{-1}, \frac{C}{M|z|} \right\}, \quad z \neq 0.$$

Therefore

$$\iint_{(\xi_1, \xi_2) \in R} |\phi(\xi_1, \xi_2)|^n d\xi_1 d\xi_2 \leq 2^{-n} \sum_{j=0}^n \binom{n}{j} \mathcal{I}_{n,j}, \quad (3.28)$$

where

$$\mathcal{I}_{n,j} := \iint_{(\xi_1, \xi_2) \in R} \psi^j(\xi_1) \psi^{n-j}(\xi_2) d\xi_1 d\xi_2 \leq \mathcal{I}_j \mathcal{I}_{n-j}; \quad (3.29)$$

$$\mathcal{I}_k := \int_{-\pi}^{\pi} \psi^k(z) dz, \quad 0 \leq k \leq n.$$

A direct integration shows that

$$\mathcal{I}_k = \begin{cases} 2\pi, & \text{if } k = 0; \\ \frac{2C}{M} + \frac{2C}{M} \log \frac{M\pi}{Ca} = O(M^{-1} \log M), & \text{if } k = 1; \\ \frac{2C}{Ma^{k-1}} + \frac{2C}{(k-1)M} \left(\left(\frac{1}{a}\right)^{k-1} - \left(\frac{C}{M\pi}\right)^{k-1} \right) = O(M^{-1} a^{-k}), & \text{if } k \geq 2. \end{cases} \quad (3.30)$$

Collecting (3.28)-(3.30), we conclude that for some constant $C' = C'(a)$, we have

$$\begin{aligned} \frac{1}{(2\pi)^2} \iint_{(\xi_1, \xi_2) \in R} |\phi(\xi_1, \xi_2)|^n d\xi_1 d\xi_2 &\leq C' 2^{-n} \left(\frac{1}{Ma^n} + \frac{\log M}{M^2 a^n} + \frac{1}{M^2 a^n} \sum_{j=2}^{n-2} \binom{n}{j} \right) \\ &= O\left(\frac{2^{-n} \gamma_n}{n}\right) + O\left(\frac{\gamma_n^2}{n}\right). \end{aligned} \quad (3.31)$$

It remains to consider the intermediate case when only one of the sines is small. Let $\mathcal{R} \subset (-\pi, \pi]^2$ be the set of points (ξ_1, ξ_2) where, for instance,

$$|2 \sin(\xi_1/2)| < b/M \quad \text{and} \quad |2 \sin(\xi_2/2)| \geq b/M.$$

This set consists of two narrow rectangles \mathcal{R}_1 and \mathcal{R}_3 , given by

$$\begin{aligned} \mathcal{R}_1 &= \{(\xi_1, \xi_2) : |\xi_1| < b_0/M \quad \text{and} \quad b_0/M \leq \xi_2 \leq \pi\}, \\ \mathcal{R}_3 &= \{(\xi_1, \xi_2) : |\xi_1| < b_0/M \quad \text{and} \quad -\pi \leq \xi_2 \leq -b_0/M\}. \end{aligned} \quad (3.32)$$

We get two more rectangles, \mathcal{R}_2 and \mathcal{R}_4 , when the sines exchange their roles. The contributions of all four rectangles are the same. Consider the rectangle \mathcal{R}_1 . We write

$$\iint_{(\xi_1, \xi_2) \in \mathcal{R}_1} \phi^n(\xi_1, \xi_2) d\xi_1 d\xi_2 = \frac{1}{2^n} \sum_{k=0}^n \binom{n}{k} \int_{-b_0/M}^{b_0/M} f^{n-k}(\xi_1) d\xi_1 \cdot \int_{b_0/M}^{\pi} f^k(\xi_2) d\xi_2, \quad (3.33)$$

and use again (3.13) and (3.14) to bound the integrals on the right. For $k \geq 1$, the second integral on the right is bounded by \mathcal{I}_k , see (3.29) and (3.30), and by (3.15), the first integral is bounded by

$$\frac{1}{M} \int_{-b_0}^{b_0} e^{-C_1(n-k)y^2} dy \leq \frac{C_3}{M\sqrt{n-k}}$$

for $k \in \{1, \dots, n-1\}$, and is bounded by C'_3/M for $k = n$. Hence

$$\int_{-b_0/M}^{b_0/M} f^{n-k}(\xi_1) d\xi_1 \leq \frac{C''_3}{M\sqrt{n-k+1}} \quad (3.34)$$

for $k \in \{1, \dots, n\}$.

Then, by (3.18), the difference between the double integral in (3.33) and

$$\frac{2\pi(\pi - b_0 M^{-1})}{2^n M \sqrt{2\pi n c_M}} \cdot (1 + O(n^{-1})) \quad (3.35)$$

(which is the contribution of the term $k = 0$) is of order at most

$$\begin{aligned} \binom{n}{1} \frac{\log M}{2^n \sqrt{n} M^2} + \frac{1}{2^n M^2} \sum_{k=2}^n \frac{1}{a^k \sqrt{n-k+1}} \binom{n}{k} \\ = \frac{\sqrt{n} \log M}{2^n M^2} + O\left(\frac{1}{M^2 \sqrt{n}} \left(\frac{1+a^{-1}}{2}\right)^n\right). \end{aligned}$$

In order to bound the first term on the right, we consider two cases: either $M \leq 2^n$, in which case we bound $\log M$ by $n \log 2$, or $M > 2^n$, in which case we bound $M^{-1} \log M$ by $2^{-n}(n \log 2)$. As a consequence, the difference between the double integral in (3.33) and the expression (3.35) is of order at most

$$\frac{n^{3/2}}{M 2^{2n}} + \frac{1}{M^2 \sqrt{n}} \left(\frac{1+a^{-1}}{2}\right)^n, \quad (3.36)$$

and the total contribution of the four narrow rectangles to $\mathbb{E}[I_{n,0}^2(\mathbf{X})]$ is

$$\begin{aligned} \frac{2}{2^n M \sqrt{2\pi n c_M}} \cdot (1 + O(n^{-1})) + O\left(\frac{n^{3/2}}{M 2^{2n}}\right) + O\left(\frac{1}{M^2 \sqrt{n}} \left(\frac{1+a^{-1}}{2}\right)^n\right) \\ = \frac{2\gamma_n}{2^n} (1 + O(n^{-1})) + O(\gamma_n^2/n). \end{aligned} \quad (3.37)$$

Putting together (3.27), (3.31) and (3.37), we obtain

$$\mathbb{E}[I_{n,0}^2] = 2 (\gamma_n^2 + 2^{-n} \gamma_n) (1 + O(n^{-1})), \quad (3.38)$$

which proves (3.8) in the special case $\ell = \ell' = 0$.

To prove (3.8) for general ℓ and ℓ' , we start from (3.23) and proceed as in the derivation of (3.38), keeping track of the changes induced by the extra factors inside the integral. In the counterpart of (3.27), this just forces replacement of the term $(1 + O(n^{-1}))$ by

$$\exp\left(-\frac{\ell_1^2 + \ell_2^2}{n M^2 c_M}\right) + O(n^{-1}).$$

In the counterpart of (3.31) the change is not noticeable, since $e^{i\ell_1 \xi_1} e^{i\ell_2 \xi_2}$ has maxnorm one. Turn to the analog of (3.37), and assume first that $\ell_2 = 0$ and $\ell_1 \neq 0$. Then the contribution of the $k = 0$ term to the integral over the rectangle \mathcal{R}_1 in the analog of (3.33) is given by (3.35), with the factor $(\exp(-\ell_1^2/(2nM^2c_M)) + O(n^{-1}))$ instead of $(1 + O(n^{-1}))$. The overall contribution of the terms $k \geq 1$ remains at most of the order given in (3.36). The contribution of the rectangle \mathcal{R}_3 is exactly the same. Not so for the rectangles \mathcal{R}_2 and \mathcal{R}_4 though! Since

$$\int_{-\pi}^{\pi} e^{i\ell_1 \xi} d\xi = 0 \quad \text{for } \ell_1 \neq 0,$$

the $k = 0$ contribution to the integral over $\mathcal{R}_2 \cup \mathcal{R}_4$ is

$$\frac{1}{2^{-n}} \int_{-b_0/M}^{b_0/M} f^n(\xi_2) d\xi_2 \int_{b_0/M \leq |\xi_1| \leq \pi} e^{i\ell\xi_1} d\xi_1 = O\left(\frac{1}{2^n M^2 \sqrt{n}}\right),$$

that is of the same order as the error term in the $k = 0$ contribution to the integral over $\mathcal{R}_1 \cup \mathcal{R}_3$. Putting these results together we get

$$\mathbb{E}[I_{n,\ell} I_{n,\ell'}] = 2\gamma_n^2 \left(\exp\left(-\frac{\ell_1^2 + \ell_2^2}{nM^2 c_M}\right) + O(n^{-1}) \right) + \frac{\gamma_n}{2^n} \left(\exp\left(-\frac{\ell_1^2 + \ell_2^2}{2nM^2 c_M}\right) + O(n^{-1}) \right) \quad (3.39)$$

if either ℓ_1 or ℓ_2 (but not both) are zero. If both ℓ_1 and ℓ_2 are non-zero, the $k = 0$ contribution from all four rectangles is of the order $O\left(\frac{1}{2^n M^2 \sqrt{n}}\right)$, so that now

$$\mathbb{E}[I_{n,\ell} I_{n,\ell'}] = 2\gamma_n^2 \left(\exp\left(-\frac{\ell_1^2 + \ell_2^2}{nM^2 c_M}\right) + O(n^{-1}) \right) + O\left(\frac{\gamma_n}{n2^n}\right). \quad (3.40)$$

Combining (3.38), (3.39) and (3.40) with the observation that $\ell_1^2 + \ell_2^2 = (\ell^2 + (\ell')^2)/2$ we get

$$\begin{aligned} \mathbb{E}[I_{n,\ell} I_{n,\ell'}] &= 2\gamma_n^2 \left(\exp\left(-\frac{\ell^2 + (\ell')^2}{2nM^2 c_M}\right) + O\left(\frac{n^{-1}}{2^n \gamma_n}\right) + O(n^{-1}) \right) \\ &\quad + (\delta_{\ell+\ell',0} + \delta_{\ell-\ell',0}) \frac{\gamma_n}{2^n} \exp\left(-\frac{\ell^2 + (\ell')^2}{2nM^2 c_M}\right). \end{aligned} \quad (3.41)$$

For ℓ and ℓ' of order $O(M)$, this gives (3.8). \square

Remark. It is worth pointing out that Proposition 3.1 is a generalization of the standard local limit theorem. Indeed, let Y be the random variable σX , where X and σ are chosen uniformly in $\{1, \dots, M\}$, and $\{-1, +1\}$, respectively. Then

$$\begin{aligned} \mathbb{E}[I_{n,\ell}] &= \frac{1}{2\pi} \int_{-\pi}^{\pi} (\cos \ell x) \mathbb{E}^n(\cos(xX)) dx \\ &= \frac{1}{2\pi} \int_{-\pi}^{\pi} e^{-i\ell x} \mathbb{E} \left(\prod_{j=1}^n e^{ixY_j} \right) dx \\ &= \mathbb{P} \left(\sum_{j=1}^n Y_j = \ell \right), \end{aligned} \quad (3.42)$$

where Y_1, \dots, Y_n are independent copies of Y . Since Y has zero expectation and variance $M^2 c_M$, equation (3.7) is just a local limit theorem for the random variable Y . In a similar

way, equation (3.8) is a local limit theorem for the coupled random variables $Y^{(1)} = \sigma^{(1)}X$ and $Y^{(2)} = \sigma^{(2)}X$, where $\sigma^{(1)}$ and $\sigma^{(2)}$ are independent random variables, chosen uniformly from $\{-1, +1\}$. Note that our results are stronger than the usual local limit theorem, which corresponds to the situation where M is bounded as $n \rightarrow \infty$.

Proof of Theorem A, Theorem B outside the window, and Theorem C(i). To apply Proposition 3.1, we first observe that $Z_{n,0} = Z_n$ and $Z_{n,1} = 0$ on \mathcal{E}_n , while $Z_{n,1} = Z_n$ and $Z_{n,0} = 0$ on \mathcal{O}_n . Consequently

$$\mathbb{E}[Z_{n,0}] = \mathbb{P}(\mathcal{E}_n)\mathbb{E}(Z_n|\mathcal{E}_n) \quad \text{and} \quad \mathbb{E}[Z_{n,0}^2] = \mathbb{P}(\mathcal{E}_n)\mathbb{E}(Z_n^2|\mathcal{E}_n), \quad (3.43)$$

while

$$\mathbb{E}[Z_{n,1}] = \mathbb{P}(\mathcal{O}_n)\mathbb{E}(Z_n|\mathcal{O}_n) \quad \text{and} \quad \mathbb{E}[Z_{n,1}^2] = \mathbb{P}(\mathcal{O}_n)\mathbb{E}(Z_n^2|\mathcal{O}_n). \quad (3.44)$$

Next we note that $\mathbb{P}_n(\mathcal{E}_n) \rightarrow 1/2$ as $n \rightarrow \infty$, with an error that is exponentially small in n . Indeed, writing $\mathbb{P}(\mathcal{E}_n) = \mathbb{P}(|\{j : X_j \text{ is odd}\}| \text{ is even})$, denoting $p = \mathbb{P}(X \text{ is odd})$, and observing that $p = \frac{1}{M} \lceil M/2 \rceil$ obeys $1/2 \leq p \leq 2/3$ for $M \geq 2$, we get

$$\begin{aligned} \mathbb{P}(\mathcal{E}_n) &= \sum_{j \text{ even}} \binom{n}{j} p^j (1-p)^{n-j} = \frac{1}{2} \sum_j \binom{n}{j} p^j (1-p)^{n-j} (1 + (-1)^j) \\ &= \frac{1}{2} [1 + (1-2p)^n] = \frac{1}{2} + O(3^{-n}). \end{aligned} \quad (3.45)$$

It now follows from (3.43) – (3.45), (3.4) and the statements of Proposition 3.1 for $\ell = \ell' = 0$ and $\ell = \ell' = 1$ that

$$\mathbb{E}(Z_n|\mathcal{E}_n) = \rho_n(1 + O(n^{-1})), \quad (3.46)$$

$$\mathbb{E}(Z_n|\mathcal{O}_n) = 2\rho_n(1 + O(n^{-1})) \quad (3.47)$$

and

$$\mathbb{E}(Z_n^2|\mathcal{E}_n) = (\mathbb{E}^2(Z_n|\mathcal{E}_n) + 2\mathbb{E}(Z_n|\mathcal{E}_n))(1 + O(n^{-1})), \quad (3.48)$$

$$\mathbb{E}(Z_n^2|\mathcal{O}_n) = (\mathbb{E}^2(Z_n|\mathcal{O}_n) + 2\mathbb{E}(Z_n|\mathcal{O}_n))(1 + O(n^{-1})), \quad (3.49)$$

where

$$\rho_n = \frac{2^{n+1}}{M\sqrt{2\pi n c_M}} = 2^{n+1}\gamma_n. \quad (3.50)$$

Comparing the definitions (3.1) and (3.50) of λ_n and ρ_n , we see that $\rho_n = \Theta(2^{-\lambda_n})$, so that the condition $\lambda_n \rightarrow -\infty$ is equivalent to the condition $\rho_n \rightarrow \infty$. By the conditional version of Cauchy-Schwarz inequality, (3.46) and (3.48), we therefore get that below the window

$$\begin{aligned} \mathbb{E}(|Z_n/\rho_n - 1| | \mathcal{E}_n) &\leq \rho_n^{-1} \sqrt{\text{Var}(Z_n|\mathcal{E}_n)} + |\mathbb{E}(Z_n/\rho_n|\mathcal{E}_n) - 1| \\ &= \rho_n^{-1} \sqrt{\mathbb{E}(Z_n^2|\mathcal{E}_n) - \mathbb{E}^2(Z_n|\mathcal{E}_n)} + |\mathbb{E}(Z_n/\rho_n|\mathcal{E}_n) - 1| \\ &= O((n^{-1} + \rho_n^{-1})^{1/2}) = o(1), \end{aligned}$$

as $n \rightarrow \infty$. Therefore, on \mathcal{E}_n , $Z_n/\rho_n \rightarrow 1$ in L_1 (in mean, that is), whence in probability. In particular, on \mathcal{E}_n , whp $Z_n > 0$, whence $Z_n = \tilde{Z}_n$ and $S_n = \log_2 Z_n$. This observation and the convergence of Z_n/ρ_n imply directly that in probability

$$S_n - |\lambda_n| + \frac{1}{2} \log_2 c_M \rightarrow \frac{1}{2} \log_2(2/\pi) \quad (3.51)$$

on \mathcal{E}_n . In the same way, (3.47) and (3.49) imply that, on \mathcal{O}_n , $Z_n/\rho_n \rightarrow 2$ in mean and probability, from which we conclude that on \mathcal{O}_n ,

$$S_n - |\lambda_n| + \frac{1}{2} \log_2 c_M \rightarrow \frac{1}{2} \log_2(8/\pi) \quad (3.52)$$

in probability.

The equations (3.51) and (3.52) certainly imply that $\Delta_{S_n} := n^{-1}(S_n - |\lambda_n|)$ goes to zero in probability. And $|\Delta_{S_n}| \leq 1$, since $0 \leq S_n \leq n$ and $|\lambda_n| \leq n$. So, by the bounded convergence theorem, $\Delta_{S_n} \rightarrow 0$ in expectation as well, completing the proof of Theorem C(i), and hence the statements of Theorems A and B below the window. To see that the statements of Theorems A and B above the window follow from Proposition 3.1 as well, we use that the probability of finding a perfect partition is equal to the probability that $Z_n > 0$, which in turn is bounded above by the expectation of Z_n . But this expectation goes to zero above the window by (3.46) and (3.47). \square

Moment estimates can also be used to obtain some statements in probability on S_n and d_n , namely the ‘‘in probability’’ statements of Theorems C(ii) and D(ii) and part of those in Theorem D(iii). These are summarized in the following proposition.

Proposition 3.2.

- (i) If $\lambda_n \rightarrow \lambda \in (-\infty, \infty)$, then both d_n and S_n are bounded in probability.
- (ii) If $\lambda_n \rightarrow \infty$, then $1/(\rho_n d_n)$ is bounded in probability.

Proof. (i) Let $Z_{n, \leq \omega} = \sum_{\ell \leq \omega} Z_{n, \ell}$, and let $\omega = \omega(n) = O(M)$ be a sequence of integers which goes to infinity. Use (3.4) and both the $\ell = \ell'$ and the $\ell \neq \ell'$ relations in Proposition 3.1 to estimate sharply the first and second moments of the sum $Z_{n, \leq \omega}$. It turns out that

$$\mathbb{E}[Z_{n, \leq \omega(n)}^2] \sim \mathbb{E}^2[Z_{n, \leq \omega(n)}] \sim (\omega(n)\rho_n)^2,$$

because $\omega(n) \rightarrow \infty$. (We leave the details to the reader.) Then the Chebyshev inequality implies that, inside the window,

$$\frac{Z_{n, \leq \omega(n)}}{\omega(n)\rho_n} \rightarrow 1 \quad (3.53)$$

in probability. Observing that ρ_n is bounded away from zero inside the window, and noting that $Z_{n, \leq \omega(n)} > 0$ implies $d_n \leq \omega(n)$, the bound (3.53) proves in particular that d_n is bounded in probability. Since $Z_{n, \leq \omega(n)} > 0$ implies $\tilde{Z}_n \leq Z_{n, \leq \omega(n)}$, the bound (3.53) also implies that inside the window \tilde{Z}_n and $S_n = \log_2 \tilde{Z}_n$ are bounded in probability.

(ii) If $\lambda_n \rightarrow \infty$, then $\rho_n \rightarrow 0$. Let $\omega(n) \rightarrow \infty$ as $n \rightarrow \infty$, slowly enough so that $k_n := 1/(\rho_n \omega(n)) \rightarrow \infty$. Since $k_n \leq M$ for all sufficiently large n , we can use (3.4) and (3.7) to conclude that

$$\mathbb{P}(d_n \leq k_n) \leq \sum_{k=0}^{k_n} \mathbb{E}[Z_{n,k}] = (1 + 2k_n) \frac{\rho_n}{2} (1 + O(n^{-1})) = O(\omega^{-1}(n)), \quad (3.54)$$

implying that d_n goes to infinity at least as fast as $1/\rho_n$, which is the desired result. \square

Remark. An alternative proof for the first statement of Proposition 3.2 can be found in Section 5, where we will in fact prove the more general statement that $d_n \rho_n$ is bounded in probability as long as ρ_n is bounded, see Theorem 5.2.

4. Subcritical Distribution of Z_n .

The next theorem provides a sharp distributional result for the number of perfect partitions.

Theorem 4.1. *Assume that $\lambda_n + \log_2 n \rightarrow -\infty$. Then, for every fixed $x \in \mathbb{R}$,*

$$\lim_{n \rightarrow \infty} \mathbb{P} \left(\frac{Z_n - \rho_n}{\rho_n \delta_n} \leq x \mid \mathcal{E}_n \right) = \frac{1}{(2\pi)^{1/2}} \int_{-\infty}^x e^{-u^2/2} du, \quad (4.1)$$

$$\lim_{n \rightarrow \infty} \mathbb{P} \left(\frac{Z_n - 2\rho_n}{2\rho_n \delta_n} \leq x \mid \mathcal{O}_n \right) = \frac{1}{(2\pi)^{1/2}} \int_{-\infty}^x e^{-u^2/2} du, \quad (4.2)$$

where

$$\delta_n = \frac{\sqrt{\text{Var}[(X/M)^2]}}{2c_M \sqrt{n}}. \quad (4.3)$$

Proof of Theorem 4.1. As in Theorem 3.1, M may or may not go to ∞ as $n \rightarrow \infty$. And as before, the harder case is the case where $M \rightarrow \infty$ as $n \rightarrow \infty$. Thus, for brevity, we again confine ourselves to the case where M is larger than some M_0 determined in the course of the estimates.

We first observe that the condition $\lambda_n + \log_2 n \rightarrow -\infty$ is equivalent to the condition

$$\lim_{n \rightarrow \infty} \frac{M}{n^{-3/2} 2^n} = 0. \quad (4.4)$$

On the event \mathcal{E}_n ,

$$Z_n = Z_{n,0} = 2^n \mathbb{P}(\boldsymbol{\sigma} \cdot \mathbf{X} = 0 \mid \mathbf{X}), \quad (4.5)$$

see (3.2). Since $\boldsymbol{\sigma} \cdot \mathbf{X}$ assumes only even values on \mathcal{E}_n , we can write

$$\mathbb{P}(\boldsymbol{\sigma} \cdot \mathbf{X} = 0 \mid \mathbf{X}) = \tilde{I}_{n,0}(\mathbf{X}), \quad \text{where}$$

$$\tilde{I}_{n,0}(\mathbf{X}) := \frac{1}{\pi} \int_{-\pi/2}^{\pi/2} \prod_{j=1}^n \cos(xX_j) dx, \quad (4.6)$$

compare with (3.5). We shall see that our ability to replace $(-\pi, \pi]$ by the smaller interval is crucial for obtaining a sharp asymptotic formula for the *random* integral $\tilde{I}_{n,0}(\mathbf{X})$. By contrast, in the proof of Theorem 3.1, we obtained expressions only for the expectation and variance of $I_{n,0}(\mathbf{X})$.

Let $M_2 = M_2(\mathbf{X}) = \sum_{j=1}^n X_j^2$, and observe that, in probability,

$$\frac{M_2}{n\mathbb{E}[\mathbf{X}^2]} \rightarrow 1 \quad \text{as } n \rightarrow \infty. \quad (4.7)$$

Let A_n be the event $n^{-1}M_2/\mathbb{E}[X^2] \in [1/2, 3/2]$. Since $\mathbb{P}(A_n) \rightarrow 1$, it suffices to consider the integral in (4.6) on $\mathcal{E}_n \cap A_n$ only. As in the proof of Theorem 3.1, we break the integral into two parts, one for $|2 \sin(x/2)| \geq b/M$, and another for the remaining x 's. However, this time we select $b \in (1, \pi)$. Then $b_0 = b_0(M)$ (defined by $2 \sin(b_0/(2M)) = b/M$) satisfies $b_0 < \pi$ for all large enough M ; in fact, it is bounded away from π for M large enough. So, if $x = y/M$ and $|y| \leq b_0$, then $|xX| = |y| \cdot (X/M) \leq b_0$, that is $|xX| < \pi$ and $|xX|$ is bounded away from π for M large enough. Therefore, for those x 's and M 's, there exist $\tilde{C}, C_1 >$ such that

$$\begin{aligned} |\cos(xX)| &\leq 1 - \tilde{C}(xX)^2 = 1 - \tilde{C}y^2(X/M)^2 \\ &\leq \exp(-C_1y^2(X/M)^2). \end{aligned} \quad (4.8)$$

And if $y^* \in (0, b_0)$ is chosen small enough then for $|y| \leq y^*$

$$\begin{aligned} \cos(xX) &= \cos(y(X/M)) = 1 - \frac{y^2}{2} \cdot (X/M)^2 + O(y^4) \\ &= \exp\left(-\frac{y^2}{2} \cdot (X/M)^2 + O(y^4)\right). \end{aligned} \quad (4.9)$$

Using (4.8), (4.9), and the fact that $M_2/(n\mathbb{E}(X^2)) \geq 1/2$ on the event A_n , we get a counterpart of (3.18):

$$\begin{aligned} \frac{1}{\pi} \int_{|x| \leq b_0/M} \prod_{j=1}^n \cos(xX_j) dx &= \frac{1}{\pi M} \int_{|y| \leq n^{-1/2} \log n} (1 + O(ny^4)) \exp\left(-\frac{M_2y^2}{2M^2}\right) dy \\ &\quad + O\left(M^{-1} \int_{|y| \geq n^{-1/2} \log n} \exp(-C_1y^2 M_2/M^2) dy\right) \\ &= \left(\frac{2}{\pi M_2}\right)^{1/2} \cdot \left(1 + O(n^{-1}) + O(e^{-C_2 \log^2 n})\right) \\ &= \left(\frac{2}{\pi M_2}\right)^{1/2} \cdot (1 + O(n^{-1})). \end{aligned} \quad (4.10)$$

It remains to show that the second integral

$$J_n(\mathbf{X}) := \frac{1}{\pi} \int_{b_0/M \leq |x| \leq \pi/2} \prod_{j=1}^n \cos(xX_j) dx$$

is likely to be $o(M_2^{-1/2})$. We have

$$\mathbb{E}[J_n^2(\mathbf{X})] = \frac{1}{\pi^2} \iint_{b_0/M \leq |x_1|, |x_2| \leq \pi/2} f^n(x_1, x_2) dx_1 dx_2, \quad (4.11)$$

see (3.12) for $f(x_1, x_2)$. The integration region consists of four squares, one per quadrant, each contributing equally to the double integral. Consider the square $\{(x_1, x_2) : b_0/M \leq x_1, x_2 \leq \pi/2\}$. Here $x_1 + x_2 \geq 2b_0/M$. If $|x_1 - x_2| \geq b_0/M$ then, by (3.12) and (3.11),

$$\begin{aligned} |f(x_1, x_2)| &\leq (2M)^{-1} \left[\frac{1 + O(M^{-1})}{2b_0/M} + \frac{1}{2} \right] + (2M)^{-1} \left[\frac{1 + O(M^{-1})}{b_0/M} + \frac{1}{2} \right] \\ &= \frac{3}{4b_0} + O(M^{-1}). \end{aligned}$$

Recall that $b_0 = b_0(M) \rightarrow b$, and we can select b arbitrarily close, from below, to π . Since $3/(4\pi) < 1/4$, we can pick b to ensure that, whenever $|x_1 - x_2| \geq b_0/M$ and M is large enough, we have

$$|f(x_1, x_2)| \leq 1/4.$$

Those points in the square contribute $O(4^{-n})$ to the double integral. Note that since $3/(4\pi) < (4.188)^{-1}$, we could have selected $b < \pi$ such that

$$|f(x_1, x_2)| \leq 1/(4.18), \quad (4.12)$$

whenever $|x_1 - x_2| \geq b_0/M$. This will come handy in the proof of Theorem 5.2.

The remaining points of the square form a narrow strip, given by

$$|x_1 - x_2| \leq b_0/M, \quad 2b_0/M \leq x_1 + x_2 \leq \pi.$$

Observe that, like the rectangle defined in (3.32), this strip is far away from the ‘‘influential’’ point (π, π) . Here this is due to the restriction $x_1, x_2 \leq \pi/2$. Arguing as in (3.33)–(3.37), we see that the strip contribution is of order at most

$$\epsilon_n := \frac{1}{2^n M n^{1/2}} + \frac{1}{M^2 \sqrt{n}} \cdot \left(\frac{1 + a^{-1}}{2} \right)^n,$$

where a constant $a \in (1, b)$ can be chosen arbitrarily. Thus

$$\mathbb{E}[J_n^2(\mathbf{X})] = O(\epsilon_n + 4^{-n}), \quad (4.13)$$

and consequently $J_n(\mathbf{X})/\sqrt{\epsilon_n + 4^{-n}}$ is bounded in probability.

Therefore, invoking (4.10), with high probability on $\mathcal{E}_n \cap A_n$, $\mathbb{P}(\boldsymbol{\sigma} \cdot \mathbf{X} = 0 | \mathbf{X})$ is equal to

$$\left(\frac{2}{\pi M_2} \right)^{1/2} \left[1 + O(n^{-1}) + O \left(\omega(n) \left(\left(\frac{M n^{1/2}}{2^n} \right)^{1/2} + n^{1/4} \left(\frac{1 + a^{-1}}{2} \right)^{n/2} \right) \right) \right],$$

if $\omega(n) \rightarrow \infty$ however slowly. (An extra term $\omega(n) \frac{Mn^{1/2}}{2^n}$ due to the 4^{-n} term in (4.13) has been subsumed by $\omega(n) \sqrt{\frac{Mn^{1/2}}{2^n}}$, as $Mn^{1/2}/2^n \rightarrow 0$.) We conclude that

$$\mathbb{P}(\boldsymbol{\sigma} \cdot \mathbf{X} = 0 | \mathbf{X}) = \left(\frac{2}{\pi M_2} \right)^{1/2} (1 + O(n^{-1}) + o_p(1)). \quad (4.14)$$

Here $o_p(1)$ stands for a random variable which approaches zero in probability. More precisely, whp it is of order $O\left(\omega(n) \left(\frac{Mn^{1/2}}{2^n}\right)^{1/2}\right)$, for any $\omega(n) \rightarrow \infty$.

Note that, in deriving (4.14), we have only used that $Mn^{1/2}/2^n \rightarrow 0$. Using the slightly stronger assumption of the theorem, namely $Mn^{3/2}/2^n \rightarrow 0$, we can replace the error term $o_p(1)$ in (4.14) by $o_p(n^{-1/2})$. (Needless to say, $U_n = o_p(n^{-1/2})$ means, by definition, that $U_n/(n^{-1/2}) \rightarrow 0$ in probability.) Consequently, on $\mathcal{E}_n \cap A_n$, whence on \mathcal{E}_n itself,

$$Z_n = \frac{2^{n+1}}{\sqrt{2\pi M_2}} (1 + o_p(n^{-1/2})). \quad (4.15)$$

We use (4.15) to show that Z_n is Gaussian in the limit. To this end, let us look close at $M_2 = \sum_{j=1}^n X_j^2$. Since

$$\frac{\sum_{j=1}^n \mathbb{E}(X_j^2)^3}{\left(\text{Var}\left(\sum_{j=1}^n X_j^2\right)\right)^{3/2}} = O(n^{-1/2}),$$

we have by Lyapunov's theorem (see, e.g., [Dur]) that

$$M_2 = \sum_{j=1}^n X_j^2 = n\mathbb{E}(X^2) + \sqrt{n\text{Var}(X^2)}\mathcal{N}_n, \quad (4.16)$$

where \mathcal{N}_n is standard normal in the limit, that is

$$\lim_{n \rightarrow \infty} \mathbb{P}(\mathcal{N}_n \leq x) = \frac{1}{(2\pi)^{1/2}} \int_{-\infty}^x e^{-u^2/2} du.$$

We want to show that \mathcal{N}_n remains standard normal in the limit if it is conditioned on the event $\mathcal{E}_n = \{\sum_{j=1}^n X_j \text{ is even}\}$. First of all $\mathcal{E}_n = \{\sum_{j=1}^n X_j^2 \text{ is even}\}$, since \mathcal{E}_n happens iff the number of odd-valued X_j 's is even.

Suppose that M is bounded. Then, by the local limit theorem (see, e.g., [Dur]),

$$\sqrt{n\text{Var}(X^2)} \mathbb{P}\left(\mathcal{N}_n = \frac{\ell - n\mathbb{E}(X^2)}{\sqrt{n\text{Var}(X^2)}}\right) = \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{(\ell - n\mathbb{E}(X^2))^2}{2n\text{Var}(X^2)}\right) + o(1),$$

uniformly for all nonnegative integers ℓ . So, for fixed $a < b$,

$$\lim_{n \rightarrow \infty} \mathbb{P} \left(\{a \leq \mathcal{N}_n \leq b\} \cap \mathcal{E}_n \right) = \frac{1}{2} \cdot \frac{1}{(2\pi)^{1/2}} \int_a^b e^{-u^2/2} du,$$

so that, for a fixed x ,

$$\lim_{n \rightarrow \infty} \mathbb{P}(\mathcal{N}_n \leq x | \mathcal{E}_n) = \frac{1}{(2\pi)^{1/2}} \int_{-\infty}^x e^{-u^2/2} du,$$

as $\lim_{n \rightarrow \infty} \mathbb{P}(\mathcal{E}_n) = 1/2$.

Next, suppose that $M \rightarrow \infty$. Then

$$|\{i \leq M : i \text{ even (odd)}\}| = \frac{M}{2} + O(1),$$

and therefore

$$\begin{aligned} \mathbb{P}(\mathcal{E}_n | X_1, \dots, X_{n-1}) &= \mathbb{P} \left(X_n \text{ has parity of } \sum_{j=1}^{n-1} X_j \mid X_1, \dots, X_{n-1} \right) \\ &= \frac{1}{2} + O(M^{-1}), \end{aligned}$$

i.e. asymptotically independent from X_1, \dots, X_{n-1} . Introduce

$$\tilde{\mathcal{N}}_{n-1} = \frac{\sum_{j=1}^{n-1} X_j^2 - (n-1)\mathbb{E}(X^2)}{\sqrt{n\text{Var}(X^2)}},$$

so that $\tilde{\mathcal{N}}_{n-1}$ depends on X_1, \dots, X_{n-1} only. Then

$$\begin{aligned} \mathbb{P} \left(\{\mathcal{N}_n \leq x\} \cap \mathcal{E}_n \right) &= \mathbb{P} \left(\{\tilde{\mathcal{N}}_{n-1} + (X_n^2 - \mathbb{E}(X^2))/\sqrt{n\text{Var}(X^2)} \leq x\} \cap \mathcal{E}_n \right) \\ &\leq \mathbb{P} \left(\{\tilde{\mathcal{N}}_{n-1} \leq x + \mathbb{E}(X^2)/\sqrt{n\text{Var}(X^2)}\} \cap \mathcal{E}_n \right) \\ &= \left(\frac{1}{2} + O(M^{-1}) \right) \mathbb{P}(\tilde{\mathcal{N}}_{n-1} \leq x + \mathbb{E}(X^2)/\sqrt{n\text{Var}(X^2)}), \end{aligned}$$

and analogously

$$\mathbb{P} \left(\{\mathcal{N}_n \leq x\} \cap \mathcal{E}_n \right) \geq \left(\frac{1}{2} + O(M^{-1}) \right) \mathbb{P} \left(\tilde{\mathcal{N}}_{n-1} \leq x + (\mathbb{E}(X^2) - M^2)/\sqrt{n\text{Var}(X^2)} \right).$$

Since $X_n^2 \leq M^2 = o(\sqrt{n \text{Var}(X^2)})$ and $\tilde{\mathcal{N}}_{n-1}$ is also standard normal in the limit, these two inequalities imply that \mathcal{N}_n , conditioned on \mathcal{E}_n , is standard normal in the limit as well.

Combining this fact with (4.15) and (4.16), we obtain (4.1). Indeed, we have that on the event \mathcal{E}_n ,

$$\begin{aligned} Z_n &= \frac{2^{n+1}}{\sqrt{2\pi(n\mathbb{E}(X^2) + (n\text{Var}(X^2))^{1/2}\mathcal{N}_n)}}(1 + o_p(n^{-1/2})) \\ &= \rho_n \left(1 + \frac{\sqrt{\text{Var}(X^2)}}{n^{1/2}\mathbb{E}(X^2)}\mathcal{N}_n \right)^{-1/2} (1 + o_p(n^{-1/2})) \\ &= \rho_n \left(1 - \frac{1}{2} \frac{\sqrt{\text{Var}(X^2)}}{n^{1/2}\mathbb{E}(X^2)}\mathcal{N}_n + o_p(n^{-1/2}) \right) \\ &= \rho_n - \frac{\rho_n \sqrt{\text{Var}(X^2)}}{2n^{1/2}\mathbb{E}(X^2)}(\mathcal{N}_n + o_p(1)) \\ &= \rho_n - \rho_n \delta_n (\mathcal{N}_n + o_p(1)), \end{aligned}$$

where $\mathcal{N}_n + o_p(1)$ converges in distribution to a standard normal variable.

The relation (4.2) is proved in a similar way. \square

The proof above allows us to obtain a limiting distribution of the entropy S_n .

Theorem 4.2. *Under the condition and in the notation of Theorem 4.1, for every fixed $x \in \mathbb{R}$,*

$$\lim_{n \rightarrow \infty} \mathbb{P} \left(\frac{S_n - |\lambda_n| + \frac{1}{2} \log_2(\pi c_M/2)}{\delta_n / \log 2} \leq x \mid \mathcal{E}_n \right) = \frac{1}{(2\pi)^{1/2}} \int_{-\infty}^x e^{-u^2/2} du, \quad (4.17)$$

$$\lim_{n \rightarrow \infty} \mathbb{P} \left(\frac{S_n - |\lambda_n| + \frac{1}{2} \log_2(\pi c_M/8)}{\delta_n / \log 2} \leq x \mid \mathcal{O}_n \right) = \frac{1}{(2\pi)^{1/2}} \int_{-\infty}^x e^{-u^2/2} du. \quad (4.18)$$

So, on both \mathcal{E}_n and \mathcal{O}_n , the entropy S_n randomly fluctuates within a distance $O_p(n^{-1/2})$ about the values $|\lambda_n| - \frac{1}{2} \log_2(\pi c_M/2)$ and $|\lambda_n| - \frac{1}{2} \log_2(\pi c_M/8)$, respectively.

Proof. First of all, whp $\tilde{Z}_n = Z_n$, since $Z_n > 0$ in probability. So, by (4.15), (3.1), (4.16) and (4.3), whp on the event \mathcal{E}_n

$$S_n = \log_2 Z_n = |\lambda_n| - \frac{1}{2} \log_2(\pi c_M/2) - \frac{\delta_n}{\log 2} \mathcal{N}_n + o_p(n^{-1/2}), \quad (4.19)$$

and, likewise, whp on the event \mathcal{O}_n

$$S_n = \log_2 Z_n = |\lambda_n| - \frac{1}{2} \log_2(\pi c_M/8) - \frac{\delta_n}{\log 2} \mathcal{N}_n + o_p(n^{-1/2}). \quad (4.20)$$

The relations (4.19) and (4.20) are equivalent to (4.17) and (4.18), respectively.

5. Bounds on the Optimal Discrepancy d_n .

Theorem 5.1. *Suppose that $\lambda_n \rightarrow \infty$, and hence $\rho_n \rightarrow 0$. Then*

(a) $\lim_{n \rightarrow \infty} \mathbb{P}(Z_n = 0) = 1$

(b) *In probability, $d_n \rho_n$ is bounded away from zero; in other words, with high probability, d_n tends to infinity at least as fast as ρ_n^{-1} does.*

Proof. (a) This follows immediately from Proposition 3.1 and the fact that

$$\mathbb{P}(Z_n > 0) \leq \mathbb{E}(Z_n). \quad (5.1)$$

(b) This has already been proven in Section 3, see Proposition 3.2 (ii). \square

The next theorem shows that with high probability, the lower bound given in Theorem 5.1 is in fact the correct order of magnitude of d_n .

Theorem 5.2. *Suppose that $\liminf_{n \rightarrow \infty} \lambda_n > -\infty$. Let $r_n \rightarrow \infty$ as a power of n at most, and introduce $\Lambda_n = \lceil r_n 2^{\lambda_n} \rceil$. Denote by $Z_{n, \leq \Lambda_n}$ the total number of partitions with discrepancy Λ_n at most. Then, in probability,*

$$\lim_{n \rightarrow \infty} \frac{Z_{n, \leq \Lambda_n}}{r_n \sqrt{6/\pi}} = 1. \quad (5.3)$$

Consequently $\mathbb{P}(d_n \leq \Lambda_n) \rightarrow 1$, that is $d_n 2^{-\lambda_n}$ (and hence $d_n \rho_n$) is bounded in probability.

Proof. Suppose that the event \mathcal{E}_n happens, so that $\sum_j X_j$ is even. Then $Z_{n,k} = 0$ if k is odd, and

$$Z_{n,k} = \frac{1}{1 + \delta_{k,0}} \frac{2^n}{\pi} \int_{-\pi/2}^{\pi/2} (e^{ikx} + e^{-ikx}) \prod_{j=1}^n \cos(xX_j) dx \quad (5.4)$$

if k is even. Now

$$Z_{n, \leq \Lambda_n} = \sum_{\mu=0}^{\mu_n-1} Z_{n, 2\mu}, \quad (5.5)$$

where $\mu_n = \min\{\mu : 2\mu > \Lambda_n\}$. Observe that $\mu_n \rightarrow \infty$ as $n \rightarrow \infty$, since $\Lambda_n \rightarrow \infty$ by the assumptions of the theorem, and note that

$$\mu_n = \frac{\Lambda_n}{2} (1 + O(\Lambda_n^{-1})) = \frac{r_n M n^{1/2}}{2} (1 + O(r_n^{-1})), \quad (5.6)$$

a relation which will be used at several points in this proof.

In light of Section 2, it would seem natural to use (5.4) and (5.5) to compute the first two moments of $Z_{n, \leq \Lambda_n}$ and to show that $\mathbb{E}[Z_{n, \leq \Lambda_n}^2] \ll \mathbb{E}^2(Z_{n, \leq \Lambda_n})$. Even though $Z_{n, \leq \Lambda_n}$ is indeed concentrated around its expected value, we prove it avoiding the Chebyshev's inequality, since we have not succeeded in showing that $\text{Var}(Z_{n, \leq \Lambda_n}) \ll \mathbb{E}^2(Z_{n, \leq \Lambda_n})$ in the whole range of

Theorem 5.2. To circumvent this substantial difficulty, we use a smoothing device, inspired by [KKLO] (the proof of Theorem 3.1), and the type of Gibbs distribution on integer partitions suggested and used in [Mer1].

In the language of statistical physics, $Z_{n, \leq \Lambda_n}$ is the zero-temperature partition function of the system with maximal discrepancy Λ_n , and the smoothing device referred to above is to study its “finite-temperature” analog

$$Z_n(q) = \sum_{\mu \leq \mu_n - 1} q^{2\mu} Z_{n, 2\mu} = \sum_{\sigma: |\sigma \cdot \mathbf{X}| \leq \Lambda_n} e^{-\beta |\sigma \cdot \mathbf{X}|}. \quad (5.7)$$

Here $\beta = -\log q$ is the inverse temperature, and $|\sigma \cdot \mathbf{X}|$ is the energy of the configuration σ in the fixed random environment \mathbf{X} . In this interpretation, the minimum discrepancy d_n is the ground state energy.

The parameter q will be chosen in such a way that $q = q_n \in (0, 1)$ goes to one as $n \rightarrow \infty$. In fact, we will choose q in such a way that $q^{\mu_n} \rightarrow 1$, or equivalently that $(1 - q)\mu_n \rightarrow 0$. Then obviously

$$Z_n(q) = (1 + O((1 - q)\mu_n)) Z_{n, \leq \Lambda_n} \quad \text{and hence} \quad Z_{n, \leq \Lambda_n} = (1 + O((1 - q)\mu_n)) Z_n(q).$$

By this observation, and by (5.6), (4.7) and (3.50), in order to prove (5.3), it suffices to show that $Z_n(q)$ is asymptotic, in probability, to $2^{n+1} \mu_n (2/(\pi M_2))^{1/2}$.

In the course of the argument, we will require some additional, mutually compatible, conditions on how fast (slow) q_n should approach 1 for this asymptotic behavior of $Z_n(q)$. As in the proof of Theorem 4.1, it suffices to study $Z_n(q)$ on $\mathcal{E}_n \cap A_n$, where $A_n = \{M_2/(n\mathbb{E}[X^2]) \in [1/2, 3/2]\}$. First of all, using (5.4) (together with the corresponding relation for $Z_{n,0}$, see equations (4.5) and (4.6)), we get

$$\begin{aligned} Z_n(q) &= \frac{2^n}{\pi} \int_{-\pi/2}^{\pi/2} \left(\sum_{|\mu| < \mu_n} q^{2|\mu|} e^{i2\mu x} \right) \prod_{j=1}^n \cos(xX_j) dx \\ &= \frac{2^n}{\pi} \int_{-\pi/2}^{\pi/2} g_n(x) \prod_{j=1}^n \cos(xX_j) dx, \quad \text{where} \\ g_n(x) &:= \frac{1 - q^4 + 2q^{2(\mu_n+1)} \cos(2(\mu_n - 1)x) - 2q^{2\mu_n} \cos 2\mu_n x}{1 - 2q^2 \cos 2x + q^4}. \end{aligned} \quad (5.8)$$

The behavior of $g_n(x)$ plays a key role in the estimates. We notice that

$$|g_n(x)| \leq \frac{C}{1 - q + |x|}, \quad \forall q \in (0, 1), \quad x \in [-\pi/2, \pi/2]. \quad (5.9)$$

Indeed the denominator is at least

$$\begin{aligned} (1 - q^2)^2 + 2q^2(1 - \cos 2x) &\geq (1 - q)^2 + 4q^2 \sin^2 x \\ &\geq C_1((1 - q)^2 + x^2) \geq \frac{C_1}{2}(1 - q + |x|)^2, \end{aligned} \quad (5.10)$$

and the numerator is bounded by

$$\begin{aligned} 4(1-q) + 2|q^2 \cos(2(\mu_n - 1)x) - \cos 2\mu_n x| &\leq 8(1-q) + 2|\cos(2(\mu_n - 1)x) - \cos 2\mu_n x| \\ &\leq 8(1-q) + 8|x| = 8(1-q + |x|). \end{aligned}$$

(The inequality (5.10) would not hold for $x \in [-\pi, \pi]$.) As in the proof of Theorem 4.1, we choose $b \in (1, \pi)$ and break the integral (5.8) into two parts, for $|x| \leq b_0/M$ and $|x| \in [b_0/M, \pi/2]$, where b_0 is again defined by $2 \sin(b_0/2M) = b/M$.

We start with the case $|x| \leq b_0/M$. The numerator of $g_n(x)$ is

$$\begin{aligned} 1 - q^4 + 2q^{2(\mu_n+1)} - 2q^{2\mu_n} \\ + 2(q^{2(\mu_n+1)} - q^{2\mu_n}) \cdot (\cos(2(\mu_n - 1)x) - 1) \\ + 2q^{2\mu_n} (\cos(2(\mu_n - 1)x) - \cos 2\mu_n x). \end{aligned}$$

The second summand is $O((1-q)(\mu_n x)^2)$, the third summand is $O(\mu_n x^2)$, and the third bound is dominant since $(1-q)\mu_n \rightarrow 0$. On the other hand,

$$\begin{aligned} \alpha_n &:= 1 - q^4 + 2q^{2(\mu_n+1)} - 2q^{2\mu_n} \\ &= (1 - q^2)(1 - q^{2\mu_n} + q^2(1 - q^{2\mu_n-2})) \\ &= (4\mu_n - 2)(1 - q)^2(1 + q)(1 + O((1-q)\mu_n)) \\ &\geq C\mu_n(1 - q)^2, \end{aligned} \tag{5.11}$$

so that, for $|x| \leq b_0/M$, the numerator is $\alpha_n(1 + O(M^{-2}(1-q)^{-2}))$. This motivates the condition $M(1-q) \rightarrow \infty$. In addition, still for $|x| \leq b_0/M$,

$$\begin{aligned} 1 - 2q^2 \cos 2x + q^4 &= (1 - q^2)^2 + 2q^2(1 - \cos 2x) \\ &= [(1 - q^2)^2 + 4q^2 x^2](1 + O(M^{-2})). \end{aligned}$$

Therefore

$$g_n(x) = \frac{\alpha_n}{(1 - q^2)^2 + 4q^2 x^2} (1 + O(M^{-2}(1-q)^{-2})), \tag{5.12}$$

and we notice up front that, by (5.11),

$$\frac{\alpha_n}{(1 - q^2)^2} = (2\mu_n - 1)(1 + O(\mu_n(1 - q))). \tag{5.13}$$

For $|x| \in [(Mn^{1/2})^{-1} \log n, b_0/M]$ we use the bound (4.8) for $\prod_{j=1}^n \cos(xX_j)$ and the relations (5.12), (5.13) to estimate

$$\frac{1}{\pi} \int_{|x| \in [\log n / (Mn^{1/2}), b_0/M]} |g_n(x)| \cdot \prod_{j=1}^n |\cos(xX_j)| dx = O\left(\frac{\mu_n}{M_2^{1/2}} e^{-\tilde{C} \log^2 n}\right); \tag{5.14}$$

cf. the remainder term in (4.10), the first equation. For the dominant $x \in [-b_0/M, b_0/M]$, by (4.9) and (5.12), (5.13), the corresponding integral is at most

$$(2\mu_n - 1) \left(\frac{2}{\pi M_2} \right)^{1/2} \left[1 + O(M^{-2}(1-q)^{-2} + n^{-1} + \mu_n(1-q)) \right].$$

Since

$$\frac{\alpha_n}{(1-q^2)^2} - \frac{\alpha_n}{(1-q^2)^2 + 4q^2x^2} \leq \frac{4\alpha_n x^2}{(1-q^2)^4},$$

the lower bound for the integral is within

$$\frac{4\alpha_n}{(1-q^2)^4} \int_{-\infty}^{\infty} x^2 e^{-M_2 x^2/2} dx = O\left(\frac{\alpha_n}{(1-q^2)^4 M_2^{3/2}} \right) = O\left(\frac{\mu_n}{(1-q^2)^2 M_2^{3/2}} \right)$$

of the upper bound. Therefore

$$\begin{aligned} \frac{1}{\pi} \int_{|x| \leq (Mn^{1/2})^{-1} \log n} g_n(x) \prod_{j=1}^n \cos(xX_j) dx &= (2\mu_n - 1) \left(\frac{2}{\pi M_2} \right)^{1/2} \\ &\times \left(1 + O(M^{-2}(1-q)^{-2} + n^{-1} + \mu_n(1-q) + M_2^{-1}(1-q)^{-2}) \right). \end{aligned} \quad (5.15)$$

Recall that M_2 is of order nM^2 on A_n . So we can drop $M_2^{-1}(1-q)^{-2}$ in the remainder term expression. The relations (5.14) and (5.15) imply that

$$\begin{aligned} \frac{1}{\pi} \int_{|x| \leq b_0/M} g_n(x) \cdot \prod_{j=1}^n \cos(xX_j) dx \\ = (2\mu_n - 1) \left(\frac{2}{\pi M_2} \right)^{1/2} \left(1 + O(M^{-2}(1-q)^{-2} + n^{-1} + \mu_n(1-q)) \right). \end{aligned} \quad (5.16)$$

We are left with the integral over $|x| \geq b_0/M$. We need to show that, in probability, the corresponding integral, call it $K_n(\mathbf{X})$, is sufficiently negligible, compared to the right-hand expression in (5.16). We have

$$\mathbb{E}[K_n^2(\mathbf{X})] = \frac{1}{\pi^2} \iint_{b_0/M \leq |x_1|, |x_2| \leq \pi/2} g_n(x_1) g_n(x_2) f^n(x_1, x_2) dx_1 dx_2.$$

Consider the first quadrant $(x_1, x_2) \in Q_1 = [b_0/M, \pi/2]^2$. By (5.9),

$$|g_n(x_1) g_n(x_2)| \leq \frac{C^2}{x_1 x_2}.$$

By (4.12), we know that, for $|x_1 - x_2| \geq b_0/M$, $|f(x_1, x_2)| \leq 1/(4.18)$, if b is chosen close enough to π and M sufficiently large. Also, by (3.14),

$$f(x_1, x_2) = \frac{1}{2}(f(x_1 + x_2) + f(x_1 - x_2)) \leq \hat{C} \left(\frac{1}{M(x_1 + x_2)} + \frac{1}{M|x_2 - x_1|} \right),$$

if $x_1 \neq x_2$. Therefore the contribution of the points (x_1, x_2) such that $|x_1 - x_2| \geq b_0/M$ is of order at most

$$(4.18)^{-n} \iint_{\substack{x_1, x_2 \geq b_0/M \\ x_2 - x_1 \geq b_0/M}} |g_n(x_1)g_n(x_2)| \cdot |f(x_1, x_2)| dx_1 dx_2 \\ \leq C^2(4.18)^{-n} \iint_{\substack{y_1, y_2 \geq b_0 \\ y_2 - y_1 \geq b_0}} \frac{dy_1 dy_2}{y_1 y_2} \left(\frac{1}{y_1 + y_2} + \frac{1}{y_2 - y_1} \right) = O((4.18)^{-n}), \quad (5.17)$$

since the last integral converges.

Let $|x_1 - x_2| \leq b_0/M$. Set $\xi_1 = x_1 - x_2$, $\xi_2 = x_1 + x_2$, so that $|\xi_1| \leq b_0/M \leq \xi_2/2$. Then

$$|x_1| + |x_2| = \frac{1}{2}(|\xi_2 + \xi_1| + |\xi_2 - \xi_1|) = \xi_2, \\ |x_1 x_2| = \frac{1}{4}(\xi_2^2 - \xi_1^2) \geq \frac{3}{16}\xi_2^2,$$

and, using (5.9),

$$|g_n(x_1)g_n(x_2)| \leq \frac{C^2}{(1-q)^2 + (1-q)(|x_1| + |x_2|) + |x_1| \cdot |x_2|} \\ \leq \frac{C'}{(1-q + \xi_2)^2}.$$

Since $f(x_1, x_2) = (f(\xi_1) + f(\xi_2))/2$, the contribution of the strip

$$\{(x_1, x_2) \in [b_0/M, \pi/2]^2 : |x_1 - x_2| \leq b_0/M\} \subset \{(\xi_1, \xi_2) : |\xi_1| \leq b_0/M, \xi_2 \in [2b_0/M, \pi]\}$$

is then of order at most

$$\frac{1}{2^n} \sum_{j=0}^n \binom{n}{j} \int_{-b_0/M}^{b_0/M} f^{n-j}(\xi_1) d\xi_1 \cdot \int_{2b_0/M}^{\pi} \frac{|f(\xi_2)|^j}{(1-q + \xi_2)^2} d\xi_2, \quad (5.18)$$

see (3.33). Here $|f(\xi_2)| \leq \min\{a^{-1}, CM^{-1}\xi_2^{-1}\}$ for M sufficiently large. Now

$$\int_{2b_0/M}^{\pi} \frac{|f(\xi_2)|}{(1-q + \xi_2)^2} d\xi_2 \leq \begin{cases} O((1-q)^{-1}) & \text{if } j = 0 \\ O\left(\frac{\log(M(1-q))}{M(1-q)^2}\right) & \text{if } j = 1 \\ O\left(\frac{a^{-j}}{M(1-q)^2}\right) & \text{if } j \geq 2, \end{cases} \quad (5.19)$$

where we used $|f(\xi_2)| \leq CM^{-1}\xi_2^{-1}$ in the cases $j = 1, 2$, and, in addition, the bound $|f(\xi_2)| \leq a^{-1}$ in the case $j > 2$. So, with the help of (3.34) and (5.47), we conclude that the sum in (5.18) is of order at most

$$\frac{1}{2^n Mn^{1/2}(1-q)} + \frac{\log(M(1-q))}{2^n M^2 n^{1/2}(1-q)^2} + \frac{(1+a^{-1})^n}{2^n M^2 n^{1/2}(1-q)^2}.$$

Since $M(1-q) \rightarrow \infty$, the second error term can be absorbed into the first one, and we get

$$\mathbb{E}[K_n^2(\mathbf{X})] \leq C \left[\frac{1}{(4.18)^n} + \frac{1}{2^n Mn^{1/2}(1-q)} + \frac{(1+a^{-1})^n}{2^n M^2 n^{1/2}(1-q)^2} \right],$$

that is, with probability approaching 1, $|K_n(\mathbf{X})|$ does not exceed

$$\omega(n) \left[\frac{1}{(2.04)^n} + \frac{1}{[2^n Mn^{1/2}(1-q)]^{1/2}} + \frac{1}{M(1-q)n^{1/4}} \left(\frac{1+a^{-1}}{2} \right)^{n/2} \right], \quad (5.20)$$

if $\omega(n) \rightarrow \infty$ however slowly. For an appropriate choice of $\omega(n)$, this bound is negligible compared to $\mu_n/(Mn^{1/2})$, the exact order of the integral in (5.16), if $\mu_n/(Mn^{1/2})$ dwarfs every one of the three summands within the square brackets in (5.20). Recalling the relation (5.6), we see that the first condition is met even if r_n is simply bounded away from zero, as $(2/(2.04))^n \rightarrow 0$. So there remain two other requirements *and* the conditions

$$(1-q)\mu_n \rightarrow 0, \quad M(1-q) \rightarrow \infty.$$

Recalling that $2^{-\lambda_n} = 2^n/(n^{1/2}M)$ is bounded by the assumptions of the theorem, we pick $\sigma > 0$ and define q by

$$\frac{Mn^{1/2}}{2^n}(1-q) = r_n^{-\sigma} \quad \text{that is} \quad q = 1 - \frac{2^n r_n^{-\sigma}}{Mn^{1/2}}. \quad (5.21)$$

Certainly $q < 1$ and $q \rightarrow 1$ as $n \rightarrow \infty$. (Here is the first spot where we use $r_n \rightarrow \infty$.) Also

$$\mu_n(1-q) = r_n \cdot \frac{Mn^{1/2}}{2^n}(1-q) = r_n^{1-\sigma} \rightarrow 0,$$

if $\sigma > 1$. Furthermore

$$M(1-q) = \frac{2^n r_n^{-\sigma}}{n^{1/2}} \rightarrow \infty,$$

if, for instance, r_n does not grow faster than $2^{n/\sigma'}$, $\sigma' > \sigma$. So it remains to guarantee that

$$\frac{\mu_n}{Mn^{1/2}} \gg \frac{1}{[2^n Mn^{1/2}(1-q)]^{1/2}} \quad (5.22)$$

and

$$\frac{\mu_n}{Mn^{1/2}} \gg \frac{(1+a^{-1})^{n/2}}{[2^n M^2 n^{1/2} (1-q)^2]^{1/2}}. \quad (5.23)$$

Using (5.6) and (5.21), we transform (5.22) into $r_n \gg r_n^{\sigma/2}$. Since $r_n \rightarrow \infty$, we can meet the condition if we choose $\sigma < 2$. (Again, a weaker condition “ r_n is bounded away from zero” would not have allowed us to find a suitable σ .) Thus we need to have $\sigma \in (1, 2)$. Finally, the condition (5.23) can be rewritten as

$$r_n^{2-2\sigma} \gg n^{1/2} \left(\frac{1+a^{-1}}{2} \right)^n,$$

and it is met if

$$r_n \leq \left(\frac{2}{1+a^{-1}} \right)^{n/(2\tilde{\sigma}-2)}, \quad \tilde{\sigma} > \sigma.$$

If r_n grows as a power of n at most, then the ratio of the square bracket expression in (5.20) and $\mu_n/(Mn^{1/2})$ is of order $r_n^{-(1-\sigma/2)}$ at most. And the “big O ”-term in (5.16) is of order $n^{-1} + r_n^{-(\sigma-1)}$ at most. Hence, choosing $\sigma = 4/3$, we obtain an asymptotic formula for $Z_n(q)$ on $\mathcal{E}_n \cap A_n$:

$$Z_n(q) = (1 + O(r_n^{-1/3} + n^{-1})) \cdot 2^n (2\mu_n - 1) \left(\frac{2}{\pi M_2} \right)^{1/2}. \quad (5.24)$$

Therefore

$$\begin{aligned} Z_{n, \leq \Lambda_n} &= (1 + O((1-q)\mu_n)) Z_n(q) \\ &= (1 + O(r_n^{-1/3} + n^{-1})) \cdot 2^n (2\mu_n - 1) \left(\frac{2}{\pi M_2} \right)^{1/2} \\ &= (1 + O(r_n^{-1/3} + n^{-1})) \cdot 2^{n+1} \mu_n \left(\frac{2}{\pi M_2} \right)^{1/2}, \end{aligned} \quad (5.25)$$

where in the last step we used that by the assumptions of the theorem $\mu_n^{-1} = O(r_n^{-1})$. Since $2\mu_n \sim \Lambda_n$, and $M_2/(3^{-1}M^2n) \rightarrow 1$ in probability, we obtain that on $\mathcal{E}_n \cap A_n$, whence on \mathcal{E}_n ,

$$\frac{Z_{n, \leq \Lambda_n}}{r_n (6/\pi)^{1/2}} \rightarrow 1$$

in probability. The same argument works for the event \mathcal{O}_n . \square

The next corollary is an immediate consequence of Theorems 5.1 and 5.2.

Corollary 5.3.

(i) If $\lim_{n \rightarrow \infty} \lambda_n \in (-\infty, \infty)$, then d_n is bounded in probability.

(ii) If $\lambda_n \rightarrow \infty$, then both $d_n \rho_n$ and $1/(d_n \rho_n)$ are bounded in probability.

Remark. From (4.16), (5.25), and (5.6) it follows that $Z_{n, \leq \Lambda_n}$ is asymptotically normal with mean $r_n \sqrt{6/\pi}$ and standard deviation $r_n \sqrt{6/(5\pi n)}$, if $r_n \gg n^{3/2}$.

6. The Distribution of d_n above the Window.

Our next theorem is a discrete counterpart of Stephan Merten's (nonrigorous) result [Mer2] on partitions of random numbers uniformly distributed on $[0, 1]$. It is formulated in terms of

$$\hat{Z}_n(t) = \frac{1}{2} \sum_{\ell \leq tb_n} Z_{n,\ell}, \quad \text{where} \quad b_n = 2^{\lambda_n+1} = \frac{M\sqrt{n}}{2^{n-1}}. \quad (6.1)$$

Note that (6.1) differs from $Z_{n,\leq tb_n}$ by a factor of two: it counts the number of unordered partitions with discrepancy at most tb_n , while $Z_{n,\leq tb_n}$ counts the number of ordered partitions with discrepancy at most tb_n .

Theorem 6.1. *Let $\lim_{n \rightarrow \infty} \lambda_n = \infty$ and $\lambda_n = O(n)$. Then the process $(\hat{Z}_n(t))$ converges, in terms of finite-dimensional distributions, to the Poisson process with parameter $(6/\pi)^{1/2}$.*

Note that the ℓ^{th} smallest discrepancy, $d_{n,\ell}$, satisfies $d_{n,\ell} \leq tb_n$ if and only if $\hat{Z}_n(t) \geq \ell$, $\ell = 1, 2, \dots$. Using this, Theorem 6.1 immediately implies the following corollary, which, in turn immediately implies that, under the conditions of Theorem 6.1, the optimum partition is unique in the limit $n \rightarrow \infty$.

Corollary. *Under the conditions of Theorem 6.1,*

$$\mathbb{P} \left\{ \frac{d_n}{b_n} > a \right\} = \mathbb{P} \{ \hat{Z}_n(a) = 0 \} \rightarrow \exp \left(-\sqrt{\frac{6}{\pi}} a \right), \quad (6.2)$$

with b_n as in (6.1). More generally, let $d_{n,r}$ denote the r^{th} smallest discrepancy. Then, for a fixed $\ell \geq 1$, the ℓ -tuple $b_n^{-1}(d_{n,1}, \dots, d_{n,\ell})$ converges (in distribution) to $(W_1, W_1 + W_2, \dots, W_1 + \dots + W_\ell)$, where W_i are i.i.d. random variables, each distributed exponentially with parameter $(6/\pi)^{1/2}$.

Remark. The condition $\lambda_n = O(n)$ is the same as “ M grows no faster than an exponential function of n ”. As was pointed out to us by the referee, one can use a coupling argument to boost the statements of Theorem 6.1 to cover arbitrary sequences $M(n)$ with $\lambda_n = \log_2 M(n) + \frac{1}{2} \log_2 n - n \rightarrow \infty$, thus giving Theorem D(iii) in the form stated in Section 2. The details of this argument are given at the end of this section.

Proof of Theorem 6.1. We will use the method of factorial moments to prove that $\hat{Z}_n = \hat{Z}_n(a)$ is asymptotically Poisson with parameter $\chi = a(6/\pi)^{1/2}$, i.e., we will show that for every integer $k \geq 1$

$$\lim_{n \rightarrow \infty} \mathbb{E} \left[(\hat{Z}_n)_k \right] = \chi^k, \quad (6.3)$$

where $(\hat{Z}_n)_k$ stands for the falling factorial $[\hat{Z}_n(\hat{Z}_n - 1) \cdots (\hat{Z}_n - k + 1)]$.

To prove that the process $(\hat{Z}_n(t))$ converges to the Poisson process with parameter $(6/\pi)^{1/2}$, one has to show that for every finite family of nonoverlapping intervals $[a_i, b_i]$, $(1 \leq i \leq r)$, the increments $\hat{Z}_n(b_i) - \hat{Z}_n(a_i)$ converge in distribution to the increments of the Poisson process

with parameter $(6/\pi)^{1/2}$. Generalizing the proof below, this is easily done by proving the convergence of the corresponding *multidimensional* factorial moments, i.e. by proving that for any fixed r -tuple (k_1, \dots, k_r) ,

$$\lim_{n \rightarrow \infty} \mathbb{E} \left[\prod_{i=1}^r (\hat{Z}_n(b_i) - \hat{Z}_n(a_i))_{k_i} \right] = \prod_{i=1}^r ((b_i - a_i)\chi)^{k_i}. \quad (6.4)$$

Since the proof of (6.4) is identical to the proof of (6.3), except for slightly more cumbersome notation, we leave it to the reader.

To prove (6.3), it is convenient to replace the random variables X_i by variables Y_i , where the variables Y_i , $i = 1, \dots, n$ are iid random variables which are equal to X_i with probability $1/2$, and equal to $-X_i$ with probability $1/2$. For every σ , (with $\sigma_1 = 1$), let I_σ denote the indicator of the event $\{|\sigma \cdot \mathbf{Y}| \leq ab_n\}$. It is then easy to see that, in terms of the random variables Y_i , $\hat{Z}_n = \hat{Z}_n(a)$ can be rewritten as $\hat{Z}_n = \sum_{\sigma} I_\sigma$.

Starting with the case $k = 1$, let us first observe that, by symmetry of Y 's, $\sigma \cdot \mathbf{Y}$ has the same distribution as $\sum_{j=1}^n Y_j$. So

$$\mathbb{E} \hat{Z}_n = 2^{n-1} \mathbb{P} \left(\left| \sum_{j=1}^n Y_j \right| \leq ab_n \right). \quad (6.5)$$

Observing that $ab_n = aM2^{1-n}\sqrt{n} = O(M)$, we now use (3.42) in conjunction with Proposition 3.1, the definition (3.6) of γ_n and the fact that $c_M = 1/3 + O(M^{-1})$ to conclude that

$$\mathbb{P} \left(\sum_{j=1}^n Y_j = \ell \right) = \gamma_n (1 + O(n^{-1})) = \frac{\sqrt{3/(2\pi)}}{Mn^{1/2}} (1 + O(n^{-1})),$$

uniformly for $|\ell| \leq ab_n$. As a consequence

$$\mathbb{P} \left(\left| \sum_{j=1}^n Y_j \right| \leq ab_n \right) = (1 + o(1)) 2^{-(n-1)} a (6/\pi)^{1/2},$$

and

$$\mathbb{E} \hat{Z}_n = (1 + o(1)) a (6/\pi)^{1/2}.$$

Next

$$\begin{aligned} \mathbb{E} \left[(\hat{Z}_n)_k \right] &= \sum_{\sigma^{(1)} \neq \dots \neq \sigma^{(k)}} \mathbb{E} \left(\prod_{s=1}^k I_{\sigma^{(s)}} \right) \\ &= \sum_{\sigma^{(1)} \neq \dots \neq \sigma^{(k)}} \sum_{|\ell^{(1)}|, \dots, |\ell^{(k)}| \leq ab_n} \mathbb{P} \left(\bigcap_{s=1}^k \{ \sigma^{(s)} \cdot \mathbf{Y} = \ell^{(s)} \} \right). \end{aligned} \quad (6.6)$$

(Since each $\boldsymbol{\sigma} \cdot \mathbf{Y}$ has parity of $\sum_{j=1}^n Y_j$, the last probability can be different from zero only if $\ell^{(1)}, \dots, \ell^{(k)}$ are either all odd, or all even.)

As a first step we will show that the leading contribution to (6.6) comes from the terms where the vectors $\boldsymbol{\sigma}^{(1)} \dots \boldsymbol{\sigma}^{(k)}$ are linear independent. To this end, let $1 \leq r \leq k$ be the rank of the $k \times n$ matrix $[\sigma_j^{(s)}]_{\{s \leq k, j \leq n\}}$, and suppose, for instance, that it is $\boldsymbol{\sigma}^{(1)}, \dots, \boldsymbol{\sigma}^{(r)}$ which form the basis of the row space. Then obviously the innermost sum in (6.6) is upper bounded by the sum

$$\sum_{|\ell^{(1)}|, \dots, |\ell^{(r)}| \leq ab_n} \mathbb{P} \left(\bigcap_{s=1}^r \{ \boldsymbol{\sigma}^{(s)} \cdot \mathbf{Y} = \ell^{(s)} \} \right). \quad (6.7)$$

Using the r -variate inversion formula for the random vector $(\boldsymbol{\sigma}^{(1)} \cdot \mathbf{Y}, \dots, \boldsymbol{\sigma}^{(r)} \cdot \mathbf{Y})$, and the independence of Y_j 's, we have

$$\mathbb{P} \left(\bigcap_{s=1}^r \{ \boldsymbol{\sigma}^{(s)} \cdot \mathbf{Y} = \ell^{(s)} \} \right) = (2\pi)^{-r} \int_{\mathbf{x} \in T^r} \exp \left(-i \sum_{s=1}^r \ell^{(s)} x_s \right) \prod_{j=1}^n f \left(\sum_{s=1}^r x_s \sigma_j^{(s)} \right) d\mathbf{x}, \quad (6.8)$$

where $f(u) := \mathbb{E}(\cos uX)$ and T^r is the r -dimensional torus $(-\pi, \pi]^r$. If, for instance, the basis of column space of the reduced $r \times n$ matrix $[\sigma_j^{(s)}]_{\{s \leq r, j \leq n\}}$ consists, say, of the vectors $(\sigma_j^{(1)}, \dots, \sigma_j^{(r)})$, ($1 \leq j \leq r$), we substitute

$$u_j = \sum_{s=1}^r x_s \sigma_j^{(s)},$$

in the first r terms in the product over j , and bound $|f(\sum_{s=1}^r x_s \sigma_j^{(s)})|$ by 1 in the remaining $n - r$ terms. Since $|f(u)|$ is 2π -periodic, and $f(u) = O(\min\{1, (M|u|)^{-1}\})$ for $|u| \leq \pi$ (see (3.11) and (3.14)), we obtain that, rather crudely, the probability in (6.8) is of order at most

$$\left(\prod_{j=1}^r \int_A^A |f(u_j)| du_j \right) = \left(\int_{-A}^A |f(u)| du \right)^r = O(M^{-r} \log^r M), \quad (6.9)$$

where $A = r\pi$. Consequently, the sum in (6.7) is of order at most

$$(b_n M^{-1} \log M)^r = O((n^{1/2} 2^{-n} \log M)^r). \quad (6.10)$$

To continue, we need to estimate the number of terms in the first sum in (6.6) for which the rank of the $k \times n$ matrix $[\sigma_j^{(s)}]_{\{s \leq k, j \leq n\}}$ is r . Consider therefore $r < k$ linear independent row vectors $\boldsymbol{\sigma}^{(1)}, \dots, \boldsymbol{\sigma}^{(r)}$. We claim that there are at most $2^{r(k-r)}$ ways to generate the additional $(k-r)$ rows linearly dependent on them. Indeed, each such row can be expanded as

$$\boldsymbol{\sigma}^{(s)} = \sum_{t=1}^r c_{st} \boldsymbol{\sigma}^{(t)},$$

Since the rank of $[\sigma_j^{(t)}]_{\{t \leq k, j \leq n\}}$ is r , we can find an $r \times r$ submatrix of rank r , implying that the coefficients c_{s1}, \dots, c_{sr} are uniquely determined by the corresponding r -long segment of the row $\sigma^{(s)}$. Since the total number of values for this segment is 2^r , we get the claim that there are at most $2^{r(k-r)}$ ways to generate $(k-r)$ rows $\sigma^{(r+1)}, \dots, \sigma^{(k)}$ linearly dependent on $\sigma^{(1)}, \dots, \sigma^{(r)}$. As a consequence, the number of terms in the first sum in (6.6) for which the rank of the $k \times n$ matrix $[\sigma_j^{(s)}]_{\{s \leq k, j \leq n\}}$ is r grows at most like $2^{nr}2^{r(k-r)}$. Unfortunately, the bound (6.10) is not sharp enough to control this many terms.

To overcome this difficulty, we use the following trick: Given $\delta \in \{-1, 1\}^r$, let

$$n_\delta = n_\delta(\sigma^{(1)}, \dots, \sigma^{(r)}) = \left| \left\{ j \leq n : (\sigma_j^{(1)}, \dots, \sigma_j^{(r)}) = \delta \right\} \right|. \quad (6.11)$$

For a typical r -tuple $(\sigma^{(1)}, \dots, \sigma^{(r)})$ one should expect that all 2^r integers n_δ are close to $n2^{-r}$. Indeed, by considering the sequence of n independent trials, with 2^r equally likely outcomes in each trial, it is easy to show that

$$\max_{\delta} \left| n_\delta(\sigma^{(1)}, \dots, \sigma^{(r)}) - \frac{n}{2^r} \right| \leq n^{1/2} \log n, \quad (6.12)$$

for all but $2^{nr}e^{-c \log^2 n}$ r -tuples $(\sigma^{(1)}, \dots, \sigma^{(r)})$. We then split the contribution of the k tuples $\sigma^{(1)}, \dots, \sigma^{(k)}$ with $r < k$ into the sum of terms for which the condition (6.12) is violated, and the sum of terms for which it is satisfied. Using the bound (6.10) and the fact that there are at most $2^{r(k-r)}$ ways to generate $(k-r)$ rows that are linearly dependent on r linear independent rows $(\sigma^{(1)}, \dots, \sigma^{(r)})$, we see that the total contribution of the k tuples $\sigma^{(1)}, \dots, \sigma^{(k)}$ with $r < k$ such that the condition (6.12) is not satisfied, is of order at most

$$(n^{1/2}2^{-n} \log M)^r \cdot 2^{nr}e^{-c \log^2 n} \cdot 2^{r(k-r)} \rightarrow 0,$$

since $\log M = O(n)$.

Suppose, on the other hand, that the $r < k$ linearly independent rows $\sigma^{(1)}, \dots, \sigma^{(r)}$ meet the condition (6.12). This means, in particular, that every $\delta \in \{-1, 1\}^r$ is among the columns of $[\sigma_j^{(s)}]_{\{s \leq r, j \leq n\}}$. Hence, from

$$\sigma^{(r+1)} = \sum_{t=1}^r c_{r+1,t} \sigma^{(t)},$$

it follows that $\sum_{t=1}^r c_{r+1,t} = 1$, and moreover

$$\left| \sum_{t=1}^r \pm c_{r+1,t} \right| = 1,$$

for *every* choice of pluses and minuses. These two conditions imply easily that $c_{r+1,t} = \delta_{tt_0}$ for some $1 \leq t_0 \leq r$, i.e. $\sigma^{(r+1)} = \sigma^{(t_0)}$. It contradicts the restriction $\sigma^{(1)} \neq \sigma^{(2)} \neq \dots \neq \sigma^{(k)}$ in (6.6).

We therefore have shown that, asymptotically as $n \rightarrow \infty$, we can restrict the summation in (6.6) to the tuples $(\sigma^{(1)}, \dots, \sigma^{(k)})$ such that $\sigma^{(1)}, \dots, \sigma^{(k)}$ are linearly independent. Using (6.10), we further see that the total contribution to the sum in (6.6) of the terms with $r = k$, that do not meet the condition (6.12), is of order at most

$$(n^{1/2} 2^{-n} \log M)^k \cdot 2^{nk} e^{-c \log^2 n} = n^{k/2} (\log M)^k e^{-c \log^2 n} \rightarrow 0,$$

so that we can further restrict the summation in (6.6) to the tuples $(\sigma^{(1)}, \dots, \sigma^{(k)})$ such that

$$\max_{\delta} \left| n_{\delta}(\sigma^{(1)}, \dots, \sigma^{(k)}) - \frac{n}{2^k} \right| \leq n^{1/2} \log n. \quad (6.13)$$

It is obvious that the last condition absorbs, for n large enough, the summation condition $\sigma^{(1)} \neq \dots \neq \sigma^{(k)}$. Moreover, for large n , (6.13) also implies linear independence of $\sigma^{(1)}, \dots, \sigma^{(k)}$. Indeed, for all $1 \leq \alpha \neq \beta \leq k$,

$$\begin{aligned} \sigma^{(\alpha)} \cdot \sigma^{(\beta)} &= \sum_{\{\delta \in \{-1,1\} : \delta_{\alpha} = \delta_{\beta}\}} n_{\delta}(\sigma^{(1)}, \dots, \sigma^{(k)}) - \sum_{\{\delta \in \{-1,1\} : \delta_{\alpha} \neq \delta_{\beta}\}} n_{\delta}(\sigma^{(1)}, \dots, \sigma^{(k)}) \\ &= 2^{k-1} \left(\frac{n}{2^k} + O(n^{1/2} \log n) \right) - 2^{k-1} \left(\frac{n}{2^k} + O(n^{1/2} \log n) \right) \\ &= O(n^{1/2} \log n), \end{aligned} \quad (6.14)$$

so that

$$\frac{\sigma^{(\alpha)} \cdot \sigma^{(\beta)}}{\|\sigma^{(\alpha)}\| \cdot \|\sigma^{(\beta)}\|} = O(n^{-1/2} \log n).$$

Hence the vectors $\sigma^{(1)}, \dots, \sigma^{(k)}$ are almost orthogonal, thus linearly independent! Finally, the condition (6.13) holds for all $(2^{(n-1)k})$ that is) but $2^{nk} e^{-c \log^2 n}$ k tuples $(\sigma^{(1)}, \dots, \sigma^{(k)})$.

It remains to estimate sharply the generic probability in (6.8) for $r = k$, and $(\sigma^{(1)}, \dots, \sigma^{(k)})$ meeting the condition (6.13). From the proof of Proposition 3.1 we recall that for every $\alpha > 1$ there exists $b_0 = b_0(\alpha) > 0$ such that $|f(u)| \leq \alpha^{-1}$ for $|u| \in [b_0/M, \pi]$. Then since $f(u)$ is 2π -periodic,

$$|f(u)| \leq \alpha^{-1}, \quad \text{if } \min_{\mu \text{ even}} |\mu\pi - u| \geq b_0/M. \quad (6.15)$$

If $\mathbf{x} = (x_1, \dots, x_k)$ is such that $u_j := \sum_{s=1}^k x_s \sigma_j^{(s)}$ satisfies the condition in (6.15) for *at least* one $j_0 \in [1, n]$, then (see (6.13)) we can upper bound the integrand in (6.8) by

$$\prod_{j \in A} |f(u_j)| \cdot \alpha^{-(n/2^k)(1+o(1))},$$

here $|A| = k - 1$, and $\{(\sigma_j^{(1)}, \dots, \sigma_j^{(k)})\}_{j \in A \cup \{j_0\}}$ is a basis of the column space. Therefore the contribution of such \mathbf{x} 's to the integral in (6.8) is of order at most

$$(M^{-1} \log M)^{k-1} \cdot \alpha^{-(n/2^k)(1+o(1))}.$$

Hence the overall contribution of such \mathbf{x} 's to the value $\mathbb{E}[(\hat{Z}_n)_k]$ in (6.6) is of order at most

$$2^{nk} b_n^k \cdot (M^{-1} \log M)^{k-1} \alpha^{-(n/2^k)(1+o(1))} = M 2^k (\log M)^{k-1} n^{k/2} \alpha^{-(n/2^k)(1+o(1))} = o(1),$$

provided $\alpha > 1$ is so large that, say, $M = o(\alpha^{n/2^{k+1}})$. (That such $\alpha = \alpha(k)$ exists follows from the condition that M grows no faster than an exponential function of n .) So, we can restrict the integration in (6.8) to the \mathbf{x} 's such that $u_j := \sum_{s=1}^k x_s \sigma_j^{(s)}$ satisfies the condition in (6.15) for all $j = 1, \dots, n$, or, equivalently, to the \mathbf{x} 's such that

$$\min_{\mu \text{ even}} \left| \mu \pi - \sum_{s=1}^k x_s \delta_s \right| < \frac{b_0}{M} \text{ for all } \boldsymbol{\delta} \in \{-1, +1\}^k. \quad (6.16)$$

(Note that, by the condition (6.13), we have $n_{\boldsymbol{\delta}}(\boldsymbol{\sigma}^{(1)}, \dots, \boldsymbol{\sigma}^{(k)}) > 0$ for all $\boldsymbol{\delta} \in \{-1, +1\}^k$, implying that the set of vectors $(\sigma_j^{(s)})_{s=1, \dots, k}$ is just the set of all vectors $\boldsymbol{\delta} \in \{-1, +1\}^k$.) Let R_k be the subset of T^k defined by (6.16). Clearly, R_k is open, and, for large M , it is a disjoint union of open neighborhoods of the 2^{k-1} points \mathbf{x}^0 in $\{0, \pi\}^k$ for which $|\{s : x_s^0 = \pi\}|$ is even. The neighborhood "centered" at such an \mathbf{x}^0 is given by

$$\left| \sum_{s=1}^k (x_s - x_s^0) \delta_s \right| < \frac{b_0}{M}, \quad \text{for all } \boldsymbol{\delta} \in \{-1, +1\}^k,$$

or equivalently

$$\sum_{s=1}^k |x_s - x_s^0| < \frac{b_0}{M}. \quad (6.17)$$

Furthermore

$$\sum_{s=1}^k x_s^0 \sigma_j^{(s)} \equiv 0 \pmod{2\pi}, \quad \forall 1 \leq j \leq n, \quad \sum_{s=1}^k x_s^0 \ell^{(s)} \equiv 0 \pmod{2\pi},$$

if the integers $\ell^{(1)}, \dots, \ell^{(s)}$ are all of the same parity. So the integrand in (6.8) equals 1 at every such \mathbf{x}^0 . Setting $x_s = x_s^0 + M^{-1} y_s$, $1 \leq s \leq k$, in the neighborhood (6.17) of \mathbf{x}^0 , we have

$$\prod_{j=1}^n f \left(\sum_{s=1}^k x_s \sigma_j^{(s)} \right) = \prod_{j=1}^n f \left(M^{-1} \sum_{s=1}^k y_s \sigma_j^{(s)} \right) = \prod_{\boldsymbol{\delta} \in \{-1, +1\}^k} f \left(M^{-1} \sum_{s=1}^k y_s \delta_s \right)^{n_{\boldsymbol{\delta}}}, \quad (6.18)$$

$$\exp \left(-i \sum_{s=1}^k \ell^{(s)} x_s \right) = \exp \left(-i M^{-1} \sum_{s=1}^k \ell^{(s)} y_s \right) = 1 + O(n^{1/2} 2^{-n}), \quad (6.19)$$

since $|\ell^{(s)}| = O(M n^{1/2} 2^{-n})$ and $|y_s| = O(1)$, ($1 \leq s \leq k$).

Consider, for a moment, the neighborhood of \mathbf{x}^0 in which $y(\boldsymbol{\delta}) = \sum_s y_s \delta_s$ is sufficiently small for all $\boldsymbol{\delta}$, say $|y(\boldsymbol{\delta})| \leq n^{-1/2} \log^2 n$. In such a neighborhood we use (3.16) to estimate

$$\prod_{\boldsymbol{\delta} \in \{-1, +1\}^k} f \left(M^{-1} \sum_{s=1}^k y_s \delta_s \right)^{n_{\boldsymbol{\delta}}} = \exp \left(-\frac{c_M}{2} (1 + o(1)) \sum_{\boldsymbol{\delta} \in \{-1, +1\}^k} n_{\boldsymbol{\delta}} (y(\boldsymbol{\delta}))^2 \right). \quad (6.20)$$

The sum over $\boldsymbol{\delta}$ simplifies, via (6.13) and the fact that $\sum_{\boldsymbol{\delta}} \delta_{s_1} \delta_{s_2} = 0$ if $s_1 \neq s_2$, to

$$\begin{aligned} \sum_{\boldsymbol{\delta} \in \{-1, +1\}^k} n_{\boldsymbol{\delta}} \sum_{s_1, s_2} y_{s_1} y_{s_2} \delta_{s_1} \delta_{s_2} &= n \sum_{s=1}^k y_s^2 + O \left(\sqrt{n} \log n \sum_{1 \leq s_1 < s_2 \leq k} |y_{s_1} y_{s_2}| \right) \\ &= (1 + O(n^{-1/2} \log n)) n \sum_{s=1}^k y_s^2, \end{aligned} \quad (6.21)$$

uniformly for all $\mathbf{y} = (y_1, \dots, y_k)$ in question.

If $|y(\boldsymbol{\delta})| > n^{-1/2} \log^2 n$ for at least one $\boldsymbol{\delta} \in \{-1, +1\}^k$, we use the bound (3.15) to conclude that

$$\begin{aligned} \left| \prod_{\boldsymbol{\delta} \in \{-1, +1\}^k} f \left(M^{-1} \sum_{s=1}^k y_s \delta_s \right)^{n_{\boldsymbol{\delta}}} \right| &\leq \exp \left(-C' \sum_{\boldsymbol{\delta} \in \{-1, +1\}^k} n_{\boldsymbol{\delta}} (y(\boldsymbol{\delta}))^2 \right) \\ &\leq e^{-\theta(\log n^2)} \exp \left(-\frac{C'}{2} \sum_{\boldsymbol{\delta} \in \{-1, +1\}^k} n_{\boldsymbol{\delta}} (y(\boldsymbol{\delta}))^2 \right) \\ &= e^{-\theta(\log n^2)} \exp \left(-\frac{nC'}{2} (1 + o(1)) \sum_{s=1}^k y_s^2 \right). \end{aligned} \quad (6.22)$$

Using the bounds (6.18)–(6.22) and proceeding as in the proof of (3.18), we get

$$\begin{aligned} \frac{1}{(2\pi)^k} \int_{\substack{\mathbf{x} \in T^k \\ \mathbf{x} \text{ meets (6.17)}}} \exp \left(-i \sum_{s=1}^k \ell^{(s)} x_s \right) \prod_{j=1}^n f \left(\sum_{s=1}^k x_s \sigma_j^{(s)} \right) d\mathbf{x} \\ = (1 + o(1)) \frac{1}{(2\pi M)^k} \int_{-\infty}^{\infty} \cdots \int_{-\infty}^{\infty} \exp \left(-\frac{c_M}{2} n \sum_{s=1}^k y_s^2 \right) d\mathbf{y} \\ = (1 + o(1)) \left(\frac{1}{M} \sqrt{\frac{3}{2\pi n}} \right)^k \end{aligned} \quad (6.23)$$

where we used $c_M = (1 + o(1)) \frac{1}{3}$. Adding up the total contribution of the 2^{k-1} points \mathbf{x}^0 with $|\{s : x_s^0 = \pi\}|$ even, we thus obtain that the right hand side of (6.8) is asymptotic to

$M^{-k} (3/(2\pi n))^{k/2} \cdot 2^{k-1}$, uniformly for all $\sigma^{(1)}, \dots, \sigma^{(k)}$, and $\ell^{(1)}, \dots, \ell_k$ in question. Now the total number of $\ell^{(1)}, \dots, \ell_k$ (either all odd or all even) is asymptotic to $2(2ab_n/2)^k = 2(ab_n)^k$, while the total number of $\sigma^{(1)}, \dots, \sigma^{(k)}$ meeting (6.13) is asymptotic to $2^{(n-1)k}$. Hence we arrive at

$$\mathbb{E}[(\hat{Z}_n)_k] = (1 + o(1)) \left(\frac{1}{M} \sqrt{\frac{3}{2\pi n}} \right)^k \cdot (2ab_n)^k \cdot 2^{(n-1)k} = (1 + o(1)) \left[a \sqrt{\frac{6}{\pi}} \right]^k. \quad \square$$

Having established Theorem 6.1, we now prove Theorem D(iii) and Theorem E. For the convenience of the reader, we summarize the relevant statements in the following theorem.

Theorem 6.2.

i) Let $\mathbf{U} = (U_1, \dots, U_n)$, where U_1, \dots, U_n are independent random variables, chosen uniformly at random from the interval $[0, 1]$, and let $d_n(\mathbf{U})$ be the minimal discrepancy,

$$d_n(\mathbf{U}) = \min_{\sigma \in \{-1, +1\}^n} |\sigma \cdot \mathbf{U}|. \quad (6.24)$$

More generally, let $d_{n,\ell}(\mathbf{U})$ denote the ℓ^{th} largest discrepancy. For any fixed $\ell \geq 1$, the ℓ -tuple $(2^{n-1}/\sqrt{n})(d_{n,1}(\mathbf{U}), \dots, d_{n,\ell}(\mathbf{U}))$ converges in distribution to $(W_1, W_1 + W_2, \dots, W_1 + \dots + W_\ell)$, where W_i are i.i.d. random variables, each distributed exponentially with parameter $(6/\pi)^{1/2}$.

ii) The statements of the corollary to Theorem 6.1 hold for any sequence $M(n)$ with $\lambda_n = \log_2 M(n) + \frac{1}{2} \log_2 n - n \rightarrow \infty$.

Proof. The proof of Theorem 6.2 uses a coupling argument suggested to us by the referee. Let $\mathbf{X} = (X_1, \dots, X_n)$ with $X_j = \lceil MU_j \rceil$. Then X_1, \dots, X_n are independent random variables, distributed uniformly in $\{1, \dots, M\}$. From $MU_j \leq X_j \leq MU_j + 1$ it follows that

$$\left| \frac{X_j}{M} - U_j \right| \leq \frac{1}{M}, \quad (6.25)$$

and hence

$$|d_n(\mathbf{U}) - d_n(\mathbf{X}/M)| \leq n/M. \quad (6.26)$$

Using the last bound and $d_n(\mathbf{X}/M) = d_n(\mathbf{X})/M$, we get

$$\left| \frac{d_n(\mathbf{U})}{n^{1/2}2^{n-1}} - \frac{1}{b_n} d_n(\mathbf{X}) \right| \leq \frac{\sqrt{n}2^{n-1}}{M} = O(n2^{-\lambda_n}). \quad (6.27)$$

In a similar way, we obtain that the ℓ^{th} largest discrepancy obeys a bound

$$\left| \frac{d_{n,\ell}(\mathbf{U})}{n^{1/2}2^{n-1}} - \frac{1}{b_n} d_{n,\ell}(\mathbf{X}) \right| \leq \frac{\sqrt{n}2^{n-1}}{M} = O(n2^{-\lambda_n}). \quad (6.28)$$

Now choose, say, $\lambda_n = n$. By the corollary to Theorem 6.1, the ℓ -tuple $b_n^{-1}(d_{n,1}(\mathbf{X}), \dots, d_{n,\ell}(\mathbf{X}))$ converges (in distribution) to $(W_1, W_1 + W_2, \dots, W_1 + \dots + W_\ell)$, where W_i are i.i.d. random variables, each distributed exponentially with parameter $(6/\pi)^{1/2}$. Since the error term in (6.28) goes to zero as $n \rightarrow \infty$, the statement i) follows.

To prove ii), we note that the distribution of $(2^{n-1}/\sqrt{n})(d_{n,1}(\mathbf{U}), \dots, d_{n,\ell}(\mathbf{U}))$ does not depend on M at all. So using (6.28) once more, we conclude that ii) follows from i) if, say, $\lambda_n \geq n$. If, on the other hand, $\lambda_n \rightarrow \infty$ in such a way that $\lambda_n \leq n$, then part ii) is basically the corollary to Theorem 6.1. \square

7. Distribution of \mathbf{d}_n inside the window.

From Corollary 5.3, d_n is bounded in probability when $Mn^{1/2}/2^n$ has a finite limit. We can easily adapt the argument in the last section to show that in this case d_n is distributed geometrically in the limit.

Theorem 7.1. *Let $\lim_{n \rightarrow \infty} \lambda_n = \lambda \in (-\infty, \infty)$. Then, for every $\ell \geq 1$,*

$$\lim_{n \rightarrow \infty} \mathbb{P}\{d_n \geq \ell\} = \frac{1+r}{2} r^{\ell-1}, \quad r := \exp\left(-2^{-\lambda} \sqrt{\frac{3}{2\pi}}\right). \quad (7.1)$$

In particular,

$$\mathbb{P}\{a \text{ perfect partition exists}\} \rightarrow 1 - r(r+1)/2.$$

Proof. Let $\hat{Z}_{n,d}$ stand for the total number of unordered partitions σ , ($\sigma_1 = 1$), with discrepancy d . Of course, if $\sum_j Y_j$ is even (odd), then $\hat{Z}_{n,d} = 0$ for all odd (even) d 's. We want to show that, for d 's even (odd), the random variables $\hat{Z}_{n,d}$ are in the limit independent Poissons on the event " $\sum_j Y_j$ is even (odd)." Consider the even case. Let $M \geq 2$, and $k_0, \dots, k_{\mu-1} \geq 0$ be given, with $k := \sum_{\nu} k_{\nu} > 0$. Then

$$\begin{aligned} \mathbb{E} \left([\hat{Z}_{n,0}]_{k_0} \cdots [\hat{Z}_{n,2(\mu-1)}]_{k_{\mu-1}}; \sum_j Y_j \text{ even} \right) &= \mathbb{E} \left([\hat{Z}_{n,0}]_{k_0} \cdots [\hat{Z}_{n,2(\mu-1)}]_{k_{\mu-1}} \right) \\ &= \sum_{\sigma^{(1)} \neq \dots \neq \sigma^{(k)}} \mathbb{P} \left(\bigcap_{\nu=0}^{\mu-1} \bigcap_{s=\sum_{j<\nu} k_j+1}^{\sum_{j \leq \nu} k_j} \{ \sigma^{(s)} \cdot Y = \pm 2\nu \} \right). \end{aligned} \quad (7.2)$$

For every choice of pluses and minuses, the probability in (7.2) is asymptotic to 2^{k-1} times the expression in (6.23), uniformly for all dominant $\sigma^{(1)}, \dots, \sigma^{(k)}$, i.e. those satisfying the condition (6.13). Therefore

$$\begin{aligned} \mathbb{E} \left([\hat{Z}_{n,0}]_{k_0} \cdots [\hat{Z}_{n,2(\mu-1)}]_{k_{\mu-1}}; \sum_j Y_j \text{ even} \right) &= (1 + o(1)) 2^{\sum_{\nu=1}^{\mu-1} k_{\nu}} \left(\frac{3^{1/2}}{M\sqrt{2\pi n}} \right)^k \cdot 2^{k-1} \cdot 2^{(n-1)k} \\ &\rightarrow \frac{1}{2} \left(\frac{\sqrt{3}}{2^{\lambda}\sqrt{2\pi}} \right)^{k_0} \cdot \left(\frac{2\sqrt{3}}{2^{\lambda}\sqrt{2\pi}} \right)^{\sum_{\nu=1}^{\mu-1} k_{\nu}}, \end{aligned}$$

and

$$\mathbb{E} \left([\hat{Z}_{n,0}]_{k_0} \cdots [\hat{Z}_{n,2(\mu-1)}]_{k_{\mu-1}} \left| \sum_j Y_j \text{ even} \right. \right) \rightarrow \left(\frac{\sqrt{3}}{2^\lambda \sqrt{2\pi}} \right)^{k_0} \cdot \left(\frac{2\sqrt{3}}{2^\lambda \sqrt{2\pi}} \right)^{\sum_{\nu=1}^{\mu-1} k_\nu}.$$

Therefore, on the event “ $\sum_j Y_j$ is even,” the random variables $\hat{Z}_{n,d}$, (d even), are in the limit $n \rightarrow \infty$ independent Poissons, $\hat{Z}_{n,0}$ with parameter $\sqrt{3}/(2^\lambda \sqrt{2\pi})$, and the rest with parameter $2\sqrt{3}/(2^\lambda \sqrt{2\pi})$.

In exactly the same fashion we establish that, on the event “ $\sum_j Y_j$ is odd,” the random variables $\hat{Z}_{n,d}$, (d odd), are in the limit $n \rightarrow \infty$ independent Poissons, *each* with parameter $2\sqrt{3}/(2^\lambda \sqrt{2\pi})$.

Therefore, for every $\mu > 0$,

$$\begin{aligned} \mathbb{P} \left\{ d_n \geq 2\mu \left| \sum_j Y_j \text{ even} \right. \right\} &= \mathbb{P} \left\{ \hat{Z}_{n,0} = 0, \dots, \hat{Z}_{n,2(\mu-1)} = 0 \left| \sum_j Y_j \text{ even} \right. \right\} \\ &\rightarrow \exp \left(-\frac{3^{1/2}}{2^\lambda \sqrt{2\pi}} - 2(\mu-1) \frac{3^{1/2}}{2^\lambda \sqrt{2\pi}} \right) \\ &= r^{2\mu-1}; \quad r := \exp \left(-2^{-\lambda} \sqrt{\frac{3}{2\pi}} \right). \end{aligned}$$

Likewise

$$\mathbb{P} \left\{ d_n \geq 2\mu + 1 \left| \sum_j Y_j \text{ odd} \right. \right\} \rightarrow r^{2\mu}.$$

Therefore, for every $\ell > 0$,

$$\begin{aligned} \mathbb{P}\{d_n \geq \ell\} &= \frac{1}{2} \mathbb{P} \left\{ d_n \geq \ell \left| \sum_j Y_j \text{ even} \right. \right\} + \frac{1}{2} \mathbb{P} \left\{ d_n \geq \ell \left| \sum_j Y_j \text{ odd} \right. \right\} \\ &\rightarrow \frac{1}{2} r^{\ell-1} + \frac{1}{2} r^\ell. \end{aligned}$$

It remains to notice that a perfect partition exists iff $d_n = 0$ or $d_n = 1$. \square

We close this section (and the paper) with the following theorem, which (together with Proposition 3.2 i)) directly implies Theorem C(ii). To state it, we recall that \tilde{Z}_n is the number of *ordered* partitions with discrepancy d_n .

Theorem 7.2. *Let $\nu = 2^{-\lambda} \sqrt{3/2\pi}$. Under the condition of Theorem 7.1, we have, for a fixed $t \geq 1$,*

$$\mathbb{P}\left(\frac{1}{2}\tilde{Z}_n = t \mid \mathcal{E}_n\right) \rightarrow e^{-\nu} \frac{\nu^t}{t!} + e^{-2\nu} \frac{(2\nu)^t}{t!} \cdot \frac{e^{-\nu}}{1 - e^{-2\nu}}, \quad (7.3)$$

$$\mathbb{P}\left(\frac{1}{2}\tilde{Z}_n = t \mid \mathcal{O}_n\right) \rightarrow e^{-2\nu} \frac{(2\nu)^t}{t!} \cdot \frac{1}{1 - e^{-2\nu}}. \quad (7.4)$$

In particular, on the event \mathcal{O}_n , the number of unordered optimal partitions, $\frac{1}{2}\tilde{Z}_n$, converges (in distribution) to $P(2\nu)$, where $P(\chi)$ is Poisson with parameter χ conditioned on the event $\{\text{Poisson}(\chi) \geq 1\}$; on the event \mathcal{E}_n , the distribution of $\frac{1}{2}\tilde{Z}_n$ converges to a mixture of $P(\nu)$ and $P(2\nu)$, with weights $1 - e^{-\nu}$ and $e^{-\nu}$, respectively.

Proof. The proof follows directly from the convergence of the sequence $\hat{Z}_{n,d}$ to the respective sequences of independent Poissons which was established in the proof of Theorem 7.2. \square

Acknowledgement.

It is our pleasure to thank Stephan Mertens for sharing his insights with us. We are also deeply indebted to the thoughtful referee who, in addition to many other useful comments, suggested to use the coupling argument to derive the continuous case results from our theorems on the integer partitioning problem.

REFERENCES

- [AF] Alon, N., Freiman, G., *On sums of subsets of a set of integers*, *Combinatorica* **8** (1988), 297–306.
- [BBCKW] Bollobás, B., Borgs, C., Chayes, J.T., Kim, J.-H. and Wilson, D.B., *The scaling window of the 2-SAT transition*, *Rand. Struc. Alg.* **18** (2001), 201–256.
- [BCP] Borgs, C., Chayes, J.T. and Pittel, B., *Sharp threshold and scaling window for the integer partitioning problem*.
- [Bol] Bollobás, B., *The evolution of random graphs*, *Trans. Amer. Math. Soc.* **286** (1984), 257–274.
- [CF] Chaimovich, M., Freiman, G., *Solving dense subset-sum problems by using analytical number theory*, *J. of Complexity* **5** (1989), 271–282.
- [Der] Derrida, B., *Phys. Rev. E* **24** (1981), 2613.
- [Dur] Durrett, R., *Probability: Theory and Examples* (Wadsworth and Brooks/Cole, Pacific Grove, CA, 1991).
- [ER1] Erdős, P. and Rényi, A., *On the evolution of random graphs*, *Magyar Tud. Akad. Mat. Kutató Int. Közl.* **5** (1960), 17–61.
- [ER2] Erdős, P. and Rényi, A., *On the evolution of random graphs*, *Bull. Inst. Internat. Statist.* **38** (1961), 343–347.
- [FF1] Ferreira, F.F. and Fontanari, J.F., *Probabilistic analysis of the number partitioning problem*, *J. Phys. A: Math. Gen.* **31** (1998), 3417–3428.

- [FF2] Ferreira, F.F. and Fontanari, J.F., *Statistical mechanics analysis of the continuous number partitioning problem*, Physica A **269** (1999), 54–60.
- [FK] Furst, H.L. and Kannan, R., *Succinct certificates for almost all subset sum problems*, SIAM J. on Computing **18** (1989), 550–558.
- [Fre] Freiman, G. A., *An analytical method of analysis of linear Boolean equations*, Ann. N.Y. Acad. Sci. **337** (1980), 97–102.
- [Fri] Friedgut, E., *Sharp thresholds of graph properties and the k -sat problem*, J. of the AMS **12** (1999), 1017–1054.
- [Fu] Fu, Y., in Lectures in the Science of Complexity, edited by D.L. Stein, (Addison-Wesley, Reading, MA, 1989).
- [GW] Gent, I.P. and Walsh, T., in Proc. of ECAI-96, edited by W. Wahlster (John Wiley & Sons, New York, 1996), pp. 170–174.
- [Gra] Graham, R., *Bounds on multiprocessing timing anomalies*, SIAM J. Appl. Math. **17** (1969), 416–429.
- [JKLP] Janson, S., Knuth, D., Luczak, T. and Pittel, B., *The birth of the giant component*, Rand. Struc. Alg. **4** (1994), 231–358.
- [KK] Karmarkar, N., and Karp, R.M., *The differencing method of set partitioning* (1982), Technical Report UCB/CSD 82/113, Computer Science Division (EECS), University of California, Berkeley.
- [KKLO] Karmarkar, N., Karp, R.M., Lueker, G.S. and Odlyzko, A.M., *Probabilistic analysis of optimum partitioning*, J. Appl. Prob. **23** (1986), 626–645.
- [Luc] Luczak, T., *Component behavior near the critical point of the random graph process*, Rand. Struc. Alg. **1** (1990), 287–310.
- [Lue] Lueker, G.S., *Exponentially small bounds on the expected optimum of the partition and subset sum problem*, Rand. Struc. Alg. **12** (1998), 51–62.
- [Mer1] Mertens, S., *Phase transition in the number partitioning problem*, Phys. Rev. Lett. **81** (1998), 4218–4221.
- [Mer2] Mertens, S., *Random Costs in Combinatorial Optimization*, Phys. Rev. Lett. **84** (2000), 1347–1350.
- [MZKST] Monasson, R., Zecchina, R., Kirkpatrick, S., Selman, B. and Troyansky, L., *Determining computational complexity from characteristic ‘phase transitions’*, Nature **400** (1999), 133–138.
- [Yak] Yakir, B., *The differencing algorithm LDM for partitioning: a proof of a conjecture of Karmarkar and Karp*, Math. Oper. Res. **21** (1996), 85–99.