MOD$_p$-tests, Almost Independence and Small Probability Spaces[*]

Claudia Bertram-Kretzberg and Hanno Lefmann

Lehrstuhl Informatik II, Universität Dortmund, D-44221 Dortmund, Germany
bertram/lefmann@ls2.informatik.uni-dortmund.de

Abstract

In this paper, we consider approximations of probability distributions over $\mathbb{Z}_p^n$. We present an approach to estimate the quality of approximations of probability distributions towards the construction of small probability spaces. These are used to derandomize algorithms. In contrast to results by Even, Goldreich, Luby, Nisan and Veličković [EGLNV], our methods are simple, and for reasonably small p, we get smaller sample spaces. Our considerations are motivated by a problem which was mentioned in recent work of Azar, Motwani and Naor [AMN], namely, how to construct in time polynomial in n a good approximation to the joint probability distribution of the random variables $X_1, X_2, \ldots, X_n$ where each X_i has values in $\{0,1\}$ and satisfies $X_i = 0$ with probability q and $X_i = 1$ with probability $1-q$ where q is arbitrary. Our considerations improve on results by [EGLNV] and [AMN].

1 Introduction

During the last years, techniques have been developed to minimize the number of random bits which are used by randomized algorithms. In general, these methods are such that independent random variables are replaced by some weakly dependent random variables which can be generated using fewer bits, therefore, dropping the running times of several algorithms. Alon, Babai and Itai [ABI] observed that it suffices for certain algorithms to use only pairwise independent bits instead of mutually independent ones. In general, to generate k-wise independent bits sample spaces of size only $O(n^k)$ can be used, cf. Karloff and Mansour [KM] for further details. However, for certain algorithms a large amount of independence is desirable. In view of this, Berger and Rompel [BR] showed that for several problems it suffices to consider only $(\log n)^c$-wise independence of the corresponding random variables. Small probability spaces are very desirable for derandomizing randomized algorithms. The resulting sample space which reflects the behaviour of the considered random variables, can be investigated by exhaustive search or by the method of conditional probabilities, cf. Alon and Spencer [AS], and Motwani, Naor and Naor [MNN].

Instead of looking for small probability spaces, Naor and Naor [NN] considered approximations to probability distributions. In their work, they used the notion of the *bias* of a distribution which was introduced by Vazirani [Va].

Definition 1.1: Let $X_1, X_2, \ldots, X_n$ be random variables with values in $\{0,1\}$. The *bias* of a subset $S \subseteq \{X_1, X_2, \ldots, X_n\}$ with respect to linear tests is defined by

$$|Prob[\sum_{X_i \in S} X_i \equiv 0 \bmod 2] - Prob[\sum_{X_i \in S} X_i \equiv 1 \bmod 2]| \, .$$

[*]This research was supported by the Deutsche Forschungsgemeinschaft as part of the Collaborative Research Center "Computational Intelligence" (531).

In an ϵ*-biased distribution,* each subset S of the random variables has bias at most ϵ. Clearly, for mutually independent and uniform random variables the bias is zero. Naor and Naor gave in [NN] constructions of ϵ-biased distributions where the sample space has size $poly(n, 1/\epsilon)$. A different construction based on Weil's theorem on quadratic residues was given by Peralta [Pe]. Alon, Goldreich, Håstad and Peralta gave in [AGHP] three constructions, including Peralta's construction, for ϵ-biased sample spaces $S \subseteq \mathbb{Z}_2^n$ with respect to linear tests in $\mathbb{Z}_2$ of size $O(n^2/(\epsilon^2(\log(n/\epsilon)^\delta)$ where $\delta = 1, 0$ and 2 in the third construction. Azar, Motwani and Naor [AMN] generalized the work of [AGHP] to random variables with values from arbitrary groups, in particular, for $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$, the set of residues modulo p. There, among others, they used Weil's theorem on character sums and Fourier transforms to obtain estimates on how to measure approximations to the uniform distribution over $\mathbb{Z}_p^n$. Here, we use a more elementary way to achieve this, and we obtain sharper estimates. The results from [AGHP] were applied in the paper [HPS] of Håstad, Phillips and Safra where, for a collection of polynomials over $\mathbb{Z}_p$ of degree at most two, they wanted to find the largest number of these polynomials which have a common root. Indeed, finding for this problem an approximate solution within a factor of $p - \epsilon$ for any $\epsilon > 0$ is as hard as finding the exact solution.

Besides Weil's theorem on quadratic residues, a similar behaviour of the underlying structures is given by Lindsey's inequality [BFS] or by the corresponding inequalities for Expander- respective Ramanujan graphs [LPS]. These phaenomena can be summarized under the term *Quasirandomness*, see [CGW], namely, the structures behave approximately like random, that is, show small discrepancies. From that point of view, it is natural that the combinatorial notion of *discrepancy* was taken into account with the work of Even, Goldreich, Luby, Nisan and Veličković [EGLNV]. Indeed, Alon, Bruck, Naor, Naor and Roth [ABNR] used Ramanujan graphs to construct good error-correcting codes which also yield small sample spaces for approximating the joint distribution of random variables.

Azar, Motwani and Naor stated in [AMN] the problem of finding good approximations for the joint distribution of random variables $X_1, X_2, \ldots, X_n$ with values in $\{0, 1\}$, where $X_1, X_2, \ldots, X_n$ are identically distributed, and $Prob[X_1 = 0] = 1 - Prob[X_1 = 1] = q \neq \frac{1}{2}$. Even, Goldreich, Luby, Nisan and Veličković [EGLNV] considered this problem in a general setting, namely, for independent random variables $X_1, X_2, \ldots, X_n$ with values in $\{1, 2, \ldots, m\}$ where $Prob[X_i = j] = p_{i,j}$, $1 \leq i \leq n$ and $1 \leq j \leq m$. In [EGLNV], constructions of small sample spaces were given which approximate the joint distribution of $X_1, X_2, \ldots, X_n$. To do so, they used the combinatorial notion of *discrepancy*, cf. [BC]. Let R_n be the set of all axis-aligned rectangles of the n-dimensional cube $[0, 1)^n$. For any finite set $S \subset [0, 1)^n$ and any rectangle $R \in R_n$ with volume $vol(R)$, the discrepancy of S on R_n is defined by $disc_S(R_n) = \sup_{R \in R_n} |vol(R) - |S \cap R|/|S||$.

A sample space $S \subseteq \{1, 2, \ldots, m\}^n$ is (ϵ, k)*-independent* with respect to the joint distribution of the independent random variables $X_1, X_2, \ldots, X_n$ with values in $\{1, 2, \ldots, m\}$ if for any sequence $(\alpha_{i_1}, \ldots \alpha_{i_k}) \in \{1, 2, \ldots, m\}^k$ it holds $|Prob[(X_{i_1}, X_{i_2} \ldots, X_{i_k}) = (\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_k})] - \prod_{j=1}^k p_{i_j, \alpha_{i_j}}| \leq \epsilon$. In [EGLNV], Even, Goldreich, Luby, Nisan and Veličković showed that sets S with small discrepancy, i.e., $disc_S(R_n) \leq \epsilon$, yield sample spaces which are (ϵ, k)-independent with respect to the joint distribution of random variables. Their construction has the advantage to be universal. One construction in [EGLNV] yields an (ϵ, k)-independent sample space $S \subseteq \{1, 2, \ldots, m\}^n$ of size $poly(\log n, 2^k, 1/\epsilon)$, while the other two constructions yield (ϵ, k)-independent spaces $S \subseteq \{1, 2, \ldots, m\}^n$ of size $O\left((n/\epsilon)^{\log(1/\epsilon)}\right)$ and $O\left((n/\epsilon)^{\log n}\right)$, respectively. The results of [EGLNV] were extended and applied by Chari, Rohatgi and Srinivasan [CRS].

Again using the notion of discrepancy and projections, they constructed an (ϵ, k)-independent sample space S of size $poly(\log n, 1/\epsilon, min\{2^k, k^{\log(1/\epsilon)}\})$.

The considerations in this paper are motivated by the problem from Azar, Motwani and Naor [AMN]. In contrast to the work of [EGLNV] and [CRS] where the discrepancy of axis-aligned rectangles is used, we offer a different approach for investigating approximations of probability spaces by using basic Linear Algebra. The intention behind our considerations is to give more insight towards the understanding of the underlying concepts for approximating random variables as asked for in [EGLNV].

Using our results on approximations to the uniform distribution over $\mathbb{Z}_p^n$, we show, by collapsing nonzero entries to 1, how good this strategy measures the deviation distance between these distributions. For uniformly distributed random variables and reasonably small values of p, the quality of our approximation is better than the one of [CRS] and [EGLNV], i.e., the sample spaces have size $O(p^2n^2/\epsilon^2)$. Otherwise, the quality of our approximations is comparable to that of [CRS], i.e., for identically distributed independent binary random variables $X_1, X_2, \ldots, X_n$ with $Prob[X_1 = 0] = 1 - Prob[X_1 = 1] = 1/p$ and p a prime, the size of an (ϵ, k)-independent sample space S is $O(2^{2k}p^2n^2/\epsilon^2)$. It should be mentioned that by using parity check matrices of BCH-codes as in [ABI] and [NN], in all these upper bounds for $|S|$ the n can be replaced by $k^2 \cdot \log_p n$ for $p \geq 3$ and by $k \cdot \log n$ for $p = 2$. in all these upper bounds for $|S|$.

However, for some applications our concepts seem to be more appropriate. Especially, if one wants to apply the results in circuit theory. Namely, Krause and Pudlak [KP] show by a probabilistic argument that $\{AND, OR, NOT\}$-circuits of quasipolynomial size (i.e., size $exp((\ln n)^{O(1)})$) can be realized by a threshold MOD_p-circuit of quasipolynomial size. Similarly, one can show that, say, a threshold AND-circuit can be simulated by a threshold-MOD_p-circuit. By choosing MOD_p-gates with ϵ-biased weight vectors, one can construct such threshold-MOD_p-circuits approximatively, cf. [Be].

2 (ϵ, k)-Independence

First we introduce some basic notation. Let p be a fixed prime number. Let $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ be the set of residues modulo p. For positive integers n, the set $\mathbb{Z}_p^n = \{0, 1, \ldots, p-1\}^n$ is the n-fold cartesian product of $\mathbb{Z}_p$. For sequences $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{Z}_p^n$ and $\beta = (\beta_1, \beta_2, \ldots, \beta_n) \in \mathbb{Z}_p^n$, let $< \alpha, \beta >_p \equiv \sum_{i=1}^n \alpha_i\beta_i \bmod p$ denote the inner product of α and β modulo p. Let $0^n = (0, 0, \ldots, 0)$ be the sequence of length n which has only zero entries.

We introduce some basic notions from probability theory. By a *sample space*, we will understand a subset $S \subseteq \mathbb{Z}_p^n$.

Definition 2.1: a) Let p be a prime. For a random variable X with values in $\mathbb{Z}_p$, let the *bias* of X be defined by

$$bias(X) = (p-1) \cdot \text{Prob}\,[X = 0] - \text{Prob}\,[X \neq 0]\,.$$

A random variable $X \in \mathbb{Z}_p$ is *ϵ-biased* if $|bias(X)| \leq \epsilon$.

b) The sample space $S \subseteq \mathbb{Z}_p^n$ is *ϵ-biased* with respect to MOD$_p$-tests if for each $c \in \mathbb{Z}_p$ and each sequence $\beta = (\beta_1, \beta_2, \ldots, \beta_n) \in \mathbb{Z}_p^n \backslash \{0^n\}$ the following is valid: if a sequence $X = (x_1, x_2, \ldots, x_n) \in S$ is chosen uniformly at random from S, then the random variable $(< \beta, X >_p + c \bmod p)$ is ϵ-biased.

c) For a fixed positive integer k, the sample space $S \subseteq \mathbb{Z}_p^n$ is *ϵ-biased* with respect to MOD$_p$-tests of size at most k if for each $c \in \mathbb{Z}_p$ and each sequence $\beta = (\beta_1, \beta_2, \ldots, \beta_n) \in \mathbb{Z}_p^n \backslash \{0^n\}$ where at most k entries of β are nonzero, the following is valid: if a sequence $X = (x_1, x_2, \ldots, x_n) \in S$ is chosen uniformly at random from S, then the random variable $(< \beta, X >_p + c \bmod p)$ is ϵ-biased.

d) A sample space $S \subseteq \mathbb{Z}_p^n$ is called *(ϵ, k)-independent* if for each k positions $1 \le i_1 < i_2 < \ldots < i_k \le n$ and any sequences $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_k) \in \mathbb{Z}_p^k$ and $X = (x_1, x_2, \ldots, x_n) \in S$ where X is chosen uniformly at random from S, we have

$$\left| \mathrm{Prob}\left[(x_{i_1}, x_{i_2}, \ldots, x_{i_k}) = \alpha\right] - \frac{1}{p^k} \right| \le \epsilon \; .$$

Thus, in an (ϵ, k)-independent sample space $S \subseteq \mathbb{Z}_p^n$, each fixed sequence of length k occurs as a subsequence approximately (up to ϵ) as often as it should.

In this paper, we will use heavily linear algebra. It turns out that the following set of functions is convenient for our purposes. For fixed elements $c \in \mathbb{Z}_p$ and sequences $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n), \beta = (\beta_1, \beta_2, \ldots, \beta_n) \in \mathbb{Z}_p^n$, let $\Phi_\beta^c \colon \mathbb{Z}_p^n \to \mathbb{R}$ be defined by

$$\Phi_\beta^c(\alpha) = \begin{cases} -\sqrt{p-1} & \text{if } \sum_{i=1}^n \alpha_i \beta_i + c \equiv 0 \bmod p \\ \frac{1}{\sqrt{p-1}} & \text{else.} \end{cases}$$

Essentially, the function Φ_β^c is a 'normalized' indicator function for the event $< \beta, \alpha >_p + c \equiv 0 \bmod p$. Namely, observe that

$$\sum_{c \in \mathbb{Z}_p} \Phi_\beta^c(\alpha) = -\sqrt{p-1} + (p-1) \cdot \frac{1}{\sqrt{p-1}} = 0 \; .$$

Central in our argumentation is the following Lemma which generalizes a result of Vazirani [Va] who considered the case $p = 2$, cf. [AGHP].

Lemma 2.2: Let $k \ge 1$ be a fixed positive integer. Let $S \subseteq \mathbb{Z}_p^n$ be a sample space which is ϵ-biased with respect to MOD$_p$-tests of size at most k. Then, the space S is $(2 \cdot \epsilon / p \cdot (1 - p^{-k}), k)$-independent.

An elementary proof of Lemma 2.2 using basic linear algebra is given in the appendix.

By Lemma 2.2, *MOD$_p$*-tests, i.e., linear tests, are appropriate to test (ϵ, k)-independence of sample spaces. Linear tests can be seen as tests for trying to refute randomness. As an immediate consequence of Lemma 2.2, we obtain:

Corollary 2.3: Let $S \subseteq \mathbb{Z}_p^n$ be a sample space which is ϵ-biased with respect to MOD$_p$-tests. Then, for every positive integer k, the space S is $(2 \cdot \epsilon / p \cdot (1 - p^{-k}), k)$-independent.

Next, we consider the distance of two probability distributions.

For any sequence $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_k) \in \mathbb{R}^k$ of reals, let $||\alpha||_1 = \sum_{i=1}^k |\alpha_i|$ denote the L_1-norm of α. The *distance* $d(\alpha, \beta)$ between two sequences $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_k)$ and $\beta = (\beta_1, \beta_2, \ldots, \beta_k)$ is defined by $d(\alpha, \beta) = ||\alpha - \beta||_1$. For two probability distributions D_1, D_2 on $\mathbb{Z}_p^k$ the *variation distance* of D_1 and D_2 is $||\, (D_1(x))_{x \in \mathbb{Z}_p^k} - (D_2(x))_{x \in \mathbb{Z}_{p^k}} \,||_1$.

Let $X_1, X_2, \ldots, X_n$ be random variables with values in some set Y. The *joint distribution* is the distribution on Y^n, i.e., for any sequence $(\alpha_1, \alpha_2, \ldots, \alpha_n) \in Y^n$ one is interested in the probability $Prob[(X_1, X_2, \ldots, X_n) = (\alpha_1, \alpha_2, \ldots, \alpha_n)]$.

Definition 2.4: Let $X_1, X_2, \ldots, X_n$ be random variables with values in $\mathbb{Z}_p$. For a subset $S \subseteq \{X_1, X_2, \ldots, X_n\}$ let $U(S)$ denote the uniform distribution on this subset S of random variables. Let $D(S)$ denote the joint distribution of S. Then, the random variables $X_1, X_2, \ldots, X_n$ are called *k-wise δ-dependent* if for all subsets S with $|S| \leq k$, we have

$$||D(S) - U(S)||_1 \leq \delta \ .$$

Theorem 2.5: If the random variables $X_1, X_2, \ldots, X_n$, with values in $\mathbb{Z}_p$ are ϵ-biased with respect to MOD$_p$-tests of size at most k, then they are also k-wise δ-dependent for $\delta = \epsilon \cdot p^{k/2}/\sqrt{p-1}$.

Thus, using a sample space of polynomial size, one can approximate well a $\log_p n$-wise independent uniform distribution, cf. [NN]. Theorem 2.5 strengthens a result of Azar, Motwani and Naor [AMN] where $\delta = p^k \cdot \epsilon$ was shown. The case $p = 2$ was proved by Alon, Goldreich, Håstad and Peralta [AGHP].

For $c \in \mathbb{Z}_p$ and $\beta \in \mathbb{Z}_p^k$, define

$$d_\beta^c = \sum_{\alpha \in \mathbb{Z}_p^k} \Phi_\beta^c(\alpha) \cdot p_\alpha \ .$$

For the proof of Theorem 2.5, we use the following lemma.

Lemma 2.6:

$$\sum_{\alpha \in \mathbb{Z}_p^k} p_\alpha^2 = p^{-(k+1)} \cdot \sum_{c \in \mathbb{Z}_p} \sum_{\beta \in \mathbb{Z}_p^k} (d_\beta^c)^2 \ . \tag{1}$$

Proof: We evaluate the right hand side of (1). Using (21) (from the appendix), we infer

$$\begin{aligned}
& \sum_{c \in \mathbb{Z}_p} \sum_{\beta \in \mathbb{Z}_p^k} (d_\beta^c)^2 = \sum_{c \in \mathbb{Z}_p} \sum_{\beta \in \mathbb{Z}_p^k} \left(\sum_{\alpha \in \mathbb{Z}_p^k} \Phi_\beta^c(\alpha) \cdot p_\alpha \right)^2 \\
= \ & \sum_{\alpha \in \mathbb{Z}_p^k} p_\alpha^2 \sum_{c \in \mathbb{Z}_p} \sum_{\beta \in \mathbb{Z}_p^k} \Phi_\beta^c(\alpha)^2 \\
& + \sum_{\gamma \in \mathbb{Z}_p^k} p_\gamma \sum_{c \in \mathbb{Z}_p} \sum_{\beta \in \mathbb{Z}_p^k} \sum_{\alpha \in \mathbb{Z}_p^k; \alpha \neq \gamma} \Phi_\beta^c(\alpha) \cdot \Phi_\beta^c(\gamma) \cdot p_\alpha \\
= \ & \sum_{\alpha \in \mathbb{Z}_p^k} p_\alpha^2 \cdot p^{k+1} + \sum_{\gamma \in \mathbb{Z}_p^k} p_\gamma \sum_{c \in \mathbb{Z}_p} \sum_{\beta \in \mathbb{Z}_p^k} \sum_{\alpha \in \mathbb{Z}_p^k; \alpha \neq \gamma} \Phi_\beta^c(\alpha) \cdot \Phi_\beta^c(\gamma) \cdot p_\alpha \\
= \ & p^{k+1} \cdot \sum_{\alpha \in \mathbb{Z}_p^k} p_\alpha^2
\end{aligned}$$

since we have by (19) (from the appendix) that

$$\sum_{c \in \mathbb{Z}_p} \sum_{\beta \in \mathbb{Z}_p^k} \sum_{\alpha \in \mathbb{Z}_p^k; \alpha \neq \gamma} \Phi_\beta^c(\alpha) \cdot \Phi_\beta^c(\gamma) \cdot p_\alpha = 0 \ .$$

□

Now we will prove Theorem 2.5.

Proof: First notice that by assumption and by (15) (from the appendix), we have $|d^c_\beta| \leq \epsilon/\sqrt{p-1}$. Using $\sum_{\alpha \in \mathbb{Z}_p^k} p_\alpha = 1$, we have

$$d^0_{0^k} = \sum_{\alpha \in \mathbb{Z}_p^k} \Phi^0_{0^k}(\alpha) \cdot p_\alpha = \sum_{\alpha \in \mathbb{Z}_p^k} -\sqrt{p-1} \cdot p_\alpha = -\sqrt{p-1}\,, \tag{2}$$

and for $c \neq 0$,

$$d^c_{0^k} = \sum_{\alpha \in \mathbb{Z}_p^k} \Phi^c_{0^k}(\alpha) \cdot p_\alpha = \frac{1}{\sqrt{p-1}}\,. \tag{3}$$

This implies that

$$p^{-(k+1)} \cdot \sum_{c \in \mathbb{Z}_p} (d^c_{0^k})^2 = p^{-k}\,. \tag{4}$$

Assume w.l.o.g. that $S = \{X_1, X_2, \ldots, X_k\}$. Then,

$$||D(S) - U(S)||_1 = \sum_{\alpha \in \mathbb{Z}_p^k} |p_\alpha - p^{-k}|\,.$$

To estimate this expression, we use the fact that $\sum_{\alpha \in \mathbb{Z}_p^k} p_\alpha = 1$ and the Cauchy-Schwarz inequality. Together with (1) and (4) we obtain

$$\begin{aligned}
\sum_{\alpha \in \mathbb{Z}_p^k} |p_\alpha - p^{-k}| \leq p^{\frac{k}{2}} \cdot \left(\sum_{\alpha \in \mathbb{Z}_p^k} (p_\alpha - p^{-k})^2 \right)^{\frac{1}{2}} = p^{\frac{k}{2}} \cdot \left(\sum_{\alpha \in \mathbb{Z}_p^k} p_\alpha^2 - p^{-k} \right)^{\frac{1}{2}} = \\
= p^{\frac{k}{2}} \cdot \left(p^{-(k+1)} \cdot \sum_{c \in \mathbb{Z}_p} \sum_{\beta \in \mathbb{Z}_p^k} (d^c_\beta)^2 - p^{-k} \right)^{\frac{1}{2}} = p^{\frac{k}{2}} \cdot \left(p^{-(k+1)} \cdot \sum_{c \in \mathbb{Z}_p} \sum_{\beta \in \mathbb{Z}_p^k \setminus \{0^k\}} (d^c_\beta)^2 \right)^{\frac{1}{2}} \leq \\
\leq p^{\frac{k}{2}} \cdot \left(p^{-k} \cdot (p^k - 1) \cdot \frac{\epsilon^2}{p-1} \right)^{\frac{1}{2}} < \frac{p^{\frac{k}{2}}}{\sqrt{p-1}} \cdot \epsilon\,.
\end{aligned}$$

Clearly, for any subset $S \subseteq \{X_1, X_2, \ldots, X_n\}$ with $|S| \leq k$, the same bound holds. □

3 Approximating Nonuniform Distributions

In [AMN] Azar, Motwani and Naor stated the problem to construct in time polynomial in n a good approximation to the joint distribution of the independent identically distributed random variables $X_1, X_2, \ldots, X_n$ where each X_i takes value 0 with probability $q \neq 1/2$ and value 1 with probability $1 - q$. We consider here the case $q = 1/p$ where p is a prime number. We consider random variables $Z_1, Z_2, \ldots, Z_n$ which take values in $\mathbb{Z}_p$ uniformly at random, i.e., $Prob[Z_i = j] = Prob[Z_i = k] = 1/p$ for all $j, k \in \mathbb{Z}_p$. Applying our results on ϵ-biased approximations to the joint distribution of $Z_1, Z_2, \ldots, Z_n$, we investigate what happens for the new distribution where all nonzero entries are collapsed to 1. Notice that in the unbiased case, i.e., $\epsilon = 0$, we obtain that the entry 0 occurs with probability $q = 1/p$ and the entry 1 with probability $1 - 1/p$.

Definition 3.1: Let $\bar{\gamma} = (\gamma_1, \gamma_2, \ldots, \gamma_n) \in \{0, *\}^n$ be a sequence where $*$ stands for any element from $\mathbb{Z}_p \backslash \{0\}$. A sequence $X = (x_1, x_2, \ldots, x_n) \in \mathbb{Z}_p^n$ is of *type* $\bar{\gamma}$, i.e., type$(X) = \bar{\gamma}$ if and only if it holds that $x_i = 0$ iff $\gamma_i = 0$ for $i = 1, 2, \ldots, n$. Thus, if two sequences $X, Y \in \mathbb{Z}_p^n$ are of the same type, the positions of the nonzero entries of X and Y coincide, but the entries need not be the same.

For sequences $\alpha \in \mathbb{Z}_p^n$, collapsing the nonzero entries of α to 1 yields a new sequence $\bar{\alpha} \in \{0,1\}^n$, the *reduced sequence of* α. For a sample space $S \subseteq \mathbb{Z}_p^n$, let the *reduced space* $\bar{S} \subseteq \mathbb{Z}_2^n$ (possibly a multiset) be obtained from S by identifying in any sequence $X = (x_1, x_2, \ldots, x_n) \in S$ every nonzero entry by 1.

Theorem 3.2: Let $S \subseteq \mathbb{Z}_p^n$ be a sample space which is ϵ-biased with respect to MOD_p-tests of size at most k. Then, the reduced space $\bar{S} \subseteq \mathbb{Z}_2^n$ is $\left(\epsilon \cdot 2^{k+1}/p, k\right)$-independent.

This improves on recent results in [EGLNV] (version from 2.97, Theorem 10).

Proof: Let $X = (x_1, x_2, \ldots, x_n)$ be chosen uniformly at random from S. We consider w.l.o.g. the first k positions of X, i.e., $x_1, x_2, \ldots, x_k$. For a sequence $\bar{\gamma} \in \{0, *\}^k$, let $P(\bar{\gamma})$ be the probability that $\bar{\gamma} = \text{type}(x_1, x_2, \ldots, x_k)$. Let $z(\bar{\gamma})$ be the number of components of $\bar{\gamma}$ with zero entries. Then, by (16) (from the appendix), we have

$$P(\bar{\gamma}) \;=\; \sum_{\alpha \in \mathbb{Z}_p^k; \text{type}(\alpha) = \bar{\gamma}} p_\alpha = p^{-(k+1)} \cdot \sum_{\alpha \in \mathbb{Z}_p^k; \text{type}(\alpha) = \bar{\gamma}} \; \sum_{\beta \in \mathbb{Z}_p^k} \; \sum_{c \in \mathbb{Z}_p} d_\beta^c \cdot \Phi_\beta^c(\alpha)\,.$$

First, consider the sum for $\beta = 0^k$. Let

$$P(\bar{\gamma}, 0^k) = p^{-(k+1)} \cdot \sum_{\alpha \in \mathbb{Z}_p^k; \text{type}(\alpha) = \bar{\gamma}} \; \sum_{c \in \mathbb{Z}_p} d_{0^k}^c \cdot \Phi_{0^k}^c(\alpha)\,. \tag{5}$$

Using (2) and (3), equality (5) becomes

$$\begin{aligned} P(\bar{\gamma}, 0^k) &= p^{-(k+1)} \cdot \sum_{\alpha \in \mathbb{Z}_p^k; \text{type}(\alpha) = \bar{\gamma}} \; \sum_{c \in \mathbb{Z}_p} d_{0^k}^c \cdot \Phi_{0^k}^c(\alpha) \\ &= p^{-(k+1)} \cdot \sum_{\alpha \in \mathbb{Z}_p^k; \text{type}(\alpha) = \bar{\gamma}} \left[\left(-\sqrt{p-1}\right)^2 + \frac{p-1}{(\sqrt{p-1})^2} \right] \\ &= \frac{(p-1)^{k - z(\bar{\gamma})}}{p^k}. \end{aligned} \tag{6}$$

With (5) and (6), we infer

$$\left| P(\bar{\gamma}) - \frac{(p-1)^{k-z(\bar{\gamma})}}{p^k} \right| = p^{-(k+1)} \cdot \left| \sum_{\beta \in \mathbb{Z}_p^k \backslash \{0^k\}} \; \sum_{c \in \mathbb{Z}_p} d_\beta^c \cdot \left(\sum_{\alpha \in \mathbb{Z}_p^k; \text{type}(\alpha) = \bar{\gamma}} \Phi_\beta^c(\alpha) \right) \right|\,. \tag{7}$$

Assume w.l.o.g. that the first $g = z(\bar{\gamma})$ components of $\bar{\gamma}$ have zero entries. We partition the set $\mathbb{Z}_p^k \setminus \{0^k\}$ into subsets $B_0, B_1, \ldots, B_{k-g}$, i.e., $\mathbb{Z}_p^k \setminus \{0^k\} = B_0 \uplus B_1 \uplus \ldots \uplus B_{k-g}$, where

$$B_j = \{\beta = (\beta_1, \beta_2, \ldots, \beta_k) \in \mathbb{Z}_p^k \setminus \{0^k\} \mid |\{i \mid g+1 \le i \le k \;\text{ and }\; \beta_i \not\equiv 0 \bmod p\}| = j\}\,.$$

Observe that for $j = 1, 2, \ldots, k-g$, we have

$$|B_0| = p^g - 1 \quad \text{and} \quad |B_j| = p^g \cdot \binom{k-g}{j} \cdot (p-1)^j \; .$$

Then, (7) becomes

$$\left| P(\bar{\gamma}) - \frac{(p-1)^{k-g}}{p^k} \right| = p^{-(k+1)} \cdot \left| \sum_{c \in \mathbb{Z}_p} \sum_{j=0}^{k-g} \sum_{\beta \in B_j} d^c_\beta \cdot \left(\sum_{\alpha \in \mathbb{Z}_p^k; type(\alpha)=\bar{\gamma}} \Phi^c_\beta(\alpha) \right) \right| \leq$$
$$\leq \quad p^{-(k+1)} \cdot \sum_{c \in \mathbb{Z}_p} \sum_{j=0}^{k-g} \sum_{\beta \in B_j} \left| d^c_\beta \right| \cdot \left| \sum_{\alpha \in \mathbb{Z}_p^k; type(\alpha)=\bar{\gamma}} \Phi^c_\beta(\alpha) \right| \; .$$

To estimate this sum, we consider first the expression $(\sum_{\alpha \in \mathbb{Z}_p^k; type(\alpha)=\bar{\gamma}} \Phi^c_\beta(\alpha))$. Fix some $\beta \in B_0$. Then, $< \alpha, \beta >_p \equiv 0 \bmod p$ for each $\alpha \in \mathbb{Z}_p^k$ with $type(\alpha) = \bar{\gamma}$. Thus, for $c = 0$, we have

$$\left| \sum_{\alpha \in \mathbb{Z}_p^k; type(\alpha)=\bar{\gamma}} \Phi^c_\beta(\alpha) \right| = (p-1)^{k-g} \cdot \sqrt{p-1} \; , \tag{8}$$

and, for $c \neq 0$, we obtain

$$\left| \sum_{\alpha \in \mathbb{Z}_p^k; type(\alpha)=\bar{\gamma}} \Phi^c_\beta(\alpha) \right| = (p-1)^{k-g} \cdot \frac{1}{\sqrt{p-1}} \; . \tag{9}$$

With $|d^c_\beta| \leq \epsilon / \sqrt{p-1}$, we infer that

$$\begin{aligned} & p^{-(k+1)} \cdot \sum_{c \in \mathbb{Z}_p} \sum_{\beta \in B_0} |d^c_\beta| \cdot \left| \sum_{\alpha \in \mathbb{Z}_p^k; type(\alpha)=\bar{\gamma}} \Phi^c_\beta(\alpha) \right| \\ \leq \quad & p^{-(k+1)} \cdot \frac{\epsilon}{\sqrt{p-1}} \cdot (p^g - 1) \cdot \left((p-1)^{k-g} \cdot \sqrt{p-1} + (p-1)^{k-g} \cdot \frac{p-1}{\sqrt{p-1}} \right) \\ = \quad & 2 \cdot p^{-(k+1)} \cdot \epsilon \cdot (p^g - 1) \cdot (p-1)^{k-g} \; . \end{aligned} \tag{10}$$

Next, we consider the case $\beta \in B_j$, $j \geq 1$. For given $c \in \mathbb{Z}_p$ and $\beta = (\beta_1, \beta_2, \ldots, \beta_l) \in \{1, 2, \ldots, p-1\}^l$, let $N(l;c)$ denote the number of solutions $X = (x_1, x_2, \ldots, x_l) \in (\mathbb{Z}_p \setminus \{0\})^l$ of the congruence $< \beta, X >_p + c \equiv 0 \bmod p$. If $x_1, x_2, \ldots, x_{l-1} \in \mathbb{Z}_p \setminus \{0\}$ are chosen arbitrarily, then there is a unique element $x_l \in \mathbb{Z}_p$ such that $< \beta, X >_p + c \equiv 0 \bmod p$. For $x_l = 0$, the number of solutions of the equation $< (\beta_1, \beta_2, \ldots, \beta_{l-1}), (x_1, x_2, \ldots, x_{l-1}) >_p + c \equiv 0 \bmod p$ is equal to $N(l-1;c)$. Thus, $N(l;c) = (p-1)^{l-1} - N(l-1;c)$. With $N(1;0) = 0$ and $N(1;c) = 1$ for $c \neq 0$, we obtain by induction that for $l \geq 2$ the following holds

$$N(l;0) = (p-1)^{l-1} - \sum_{i=1}^{l-2} (p-1)^i \cdot (-1)^{l+i} \; ,$$

and,

$$N(l;c) = (p-1)^{l-1} - \sum_{i=0}^{l-2} (p-1)^i \cdot (-1)^{l+i} \,.$$

For fixed $\beta_j \in B_j$, $j \geq 1$, we infer

$$\begin{aligned}
& \sum_{c \in \mathbb{Z}_p} \left| \sum_{\alpha \in \mathbb{Z}_p^k; type(\alpha)=\bar{\gamma}} \Phi_\beta^c(\alpha) \right| \\
= & \sum_{c \in \mathbb{Z}_p} \left| (p-1)^{k-g-j} \cdot N(j;c) \cdot (-\sqrt{p-1}) + \Big((p-1)^{k-g} - N(j;c) \cdot (p-1)^{k-g-j} \Big) \cdot \frac{1}{\sqrt{p-1}} \right| \\
= & \sum_{c \in \mathbb{Z}_p} (p-1)^{k-g-j} \cdot \sqrt{p-1} \cdot \left| -N(j;c) + \frac{(p-1)^j - N(j;c)}{p-1} \right| = 2 \cdot (p-1)^{k-g-j} \cdot \sqrt{p-1} \qquad (11)
\end{aligned}$$

Using $|d_\beta^c| \leq \epsilon / \sqrt{p-1}$, we obtain

$$\begin{aligned}
& p^{-(k+1)} \cdot \sum_{j=1}^{k-g} \sum_{\beta \in B_j} \sum_{c \in \mathbb{Z}_p} |d_\beta^c| \cdot \left| \sum_{\alpha \in \mathbb{Z}_p^k; type(\alpha)=\bar{\gamma}} \Phi_\beta^c(\alpha) \right| \\
\leq \; & p^{-(k+1)} \cdot \frac{\epsilon}{\sqrt{p-1}} \cdot \sum_{j=1}^{k-g} p^g \cdot \binom{k-g}{j} \cdot (p-1)^j \cdot 2 \cdot (p-1)^{k-g-j} \cdot \sqrt{p-1} \\
= \; & 2 \cdot p^{-(k+1)} \cdot \epsilon \cdot p^g \cdot (p-1)^{k-g} \cdot (2^{k-g} - 1) \,. \qquad (12)
\end{aligned}$$

Altogether, with (10) and (12), we obtain

$$\begin{aligned}
\left| P(\bar{\gamma}) - \frac{(p-1)^{k-z(\bar{\gamma})}}{p^k} \right| \; & \leq \; p^{-(k+1)} \cdot (p-1)^{k-g} \cdot \Big[2 \cdot \epsilon \cdot (p^g - 1) + 2 \cdot \epsilon \cdot p^g \cdot (2^{k-g} - 1) \Big] \\
& \leq \; \frac{\epsilon \cdot 2^{k+1}}{p} \,.
\end{aligned}$$

□

Theorem 3.3: Let $S \subseteq \mathbb{Z}_p^k$ be a sample space which is ϵ-biased with respect to MOD_p-tests of size at most k. Then, the reduced space $\bar{S} \subseteq \mathbb{Z}_2^k$ is k-wise $(\epsilon \cdot 3^k / p)$-dependent.

Thus, using a sample space of polynomial size, one can approximate well a $\log_3 n$-wise independent nonuniform distribution, cf. [NN].

Proof: Set $P(\bar{\gamma}) = \sum_{\alpha \in \mathbb{Z}_p^k; type(\alpha)=\bar{\gamma}} p_\alpha$. By assumption and (15) (from the appendix), we have $|d_\beta^c| \leq \epsilon / \sqrt{p-1}$. We have to compute $\sum_{\bar{\gamma} \in \mathbb{Z}_2^k} \left| P(\bar{\gamma}) - \frac{(p-1)^{k-z(\bar{\gamma})}}{p^k} \right|$. Using (1), (2), (3), (10) and (12), we obtain

$$\sum_{\bar{\gamma} \in \mathbb{Z}_2^k} \left| P(\bar{\gamma}) - \frac{(p-1)^{k-z(\bar{\gamma})}}{p^k} \right|$$

$$\begin{aligned}
&\leq p^{-(k+1)} \cdot \epsilon \cdot \sum_{\bar{\gamma} \in \mathbb{Z}_2^k} \left[2 \cdot (p^{z(\bar{\gamma})} - 1) \cdot (p-1)^{k-z(\bar{\gamma})} + 2 \cdot p^{z(\bar{\gamma})} \cdot (p-1)^{k-z(\bar{\gamma})} \cdot (2^{k-z(\bar{\gamma})} - 1)\right] \\
&= p^{-(k+1)} \cdot \epsilon \cdot \sum_{g=0}^{k} \binom{k}{g} \cdot \left[2 \cdot (p^g - 1) \cdot (p-1)^{k-g} + 2 \cdot p^g \cdot (p-1)^{k-g} \cdot (2^{k-g} - 1)\right] \\
&= p^{-(k+1)} \cdot \epsilon \cdot \left[2 \cdot (3p-2)^k - 2 \cdot p^k\right] \\
&< 2 \cdot p^{-(k+1)} \cdot \epsilon \cdot (3p-2)^k < \frac{\epsilon \cdot 3^k}{p}
\end{aligned}$$

which yields the desired result. □

4 Applications

Lemma 2.2 links the ability to pass MOD_p-tests with almost independence. We can use this to consider the problem of Azar, Motwani and Naor [AMN] to construct a p-ary sample space that is ϵ-biased with respect to MOD_p-tests. Starting with an ϵ-biased sample space $S \subseteq \mathbb{Z}_p^n$, according to Lemma 2.2, the space S is $(2 \cdot \epsilon/p \cdot (1 - p^{-k}), k)$-independent. If we replace in every vector of the sample space every nonzero entry by one, our sample space which might be a multiset, will become a reasonable approximation, cf. Theorem 3.2, to the distribution on n p-ary random variables in which each random variable independently takes value 0 with probability $1/p$ and 1 with probability $1 - 1/p$.

Alon, Goldreich, Håstad and Peralta gave in [AGHP] three constructions for sample spaces which are ϵ-biased with respect to linear tests. These can be modified such that they also yield sample spaces which are ϵ-biased with respect to MOD_p tests. The generalizations of two constructions to the p-ary case are due to Azar, Motwani and Naor [AMN] and to Even [Ev]. The generalization of the third construction is straightforward. For completeness and to have a typical example, we give it below. Another construction using Ramanujan graphs and Justesen codes is given in [ABNR] where an (ϵ, k)-independent sample space of size $O(n/\epsilon^3)$ is constructed.

Construction: For a fixed prime p, consider the finite field $GF(p^m)$. Let $f: GF(p^m) \longrightarrow \mathbb{Z}_p^m$ be the standard representation of $GF(p^m)$ as a vector space over $GF(p)$. Then $f(0) = 0^m$ and $f(u+v) \equiv (f(u) \oplus f(v)) \bmod p$ where addition $+$ is meant in $GF(p^m)$ and addition $\oplus$ in $\mathbb{Z}_p^m$ is meant componentwise modulo p. The sample space S_m^n is defined as follows. The elements of S_m^n are determined by pairs of elements in $GF(p^m)$, namely given two elements $x, y \in GF(p^m)$, the ith entry of the sequence $s_{x,y} \in S_m^n$ is the inner product $< f(x^i), f(y) >_p$, $i = 0, 1, \ldots, n-1$.

The sample space S_m^n has the following properties:

Proposition 4.1: The sample space S_m^n has size $|S_m^n| = p^{2m}$ and is $(p-1) \cdot (n-1)/p^m$-biased with respect to MOD_p-tests.

Proof: Clearly, we have $|S_m^n| = p^{2m}$. Let $s(x,y) = (s_0(x,y), s_1(x,y), \ldots, s_{n-1}(x,y))$ where $s_i(x,y) \equiv < f(x^i), f(y) >_p$, denote the element from S_m^n specified by $x, y \in GF(p^m)$. Note that by linearity of f for any sequence $\alpha \in \mathbb{Z}_p^n$, we have

$$< \alpha, s(x,y) >_p \equiv \sum_{i=0}^{n-1} \alpha_i \cdot < f(x^i), f(y) >_p \equiv < f(\sum_{i=0}^{n-1} \alpha_i \cdot x^i), f(y) >_p \ .$$

Let $p_\alpha(t) = \sum_{i=0}^{n-1} \alpha_i \cdot t^i$ be a polynomial over $\mathbb{Z}_p$ which is not identically zero. We want to determine the distribution of $< f(p_\alpha(x)), f(y) >_p$ where $x \in GF(p^m)$ and $y \in GF(p^m)$ are chosen uniformly at random. To do so, we first fix $x \in GF(p^m)$. We distinguish two cases:

1) Assume that $p_\alpha(x) \neq 0$, i.e., x is not a zero of $p_\alpha(t)$. Then, $f(p_\alpha(x)) \neq 0^m$ and for uniformly chosen $y \in GF(p^m)$, the values $< f(p_\alpha(x)), f(y) >_p$ are as well uniformly distributed in $\mathbb{Z}_p$, that is $< f(p_\alpha(x)), f(y) >_p$ is unbiased.

2) If $p_\alpha(x) = 0$, then $< f(p_\alpha(x)), f(y) >_p \equiv 0 \bmod p$ for all $y \in GF(p^m)$. However, the polynomial $p_\alpha(t)$ has at most $n-1$ zeros.

Therefore, for each $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{Z}_p^n$ where the polynomial $p_\alpha(t) = \sum_{i=0}^{n-1} \alpha_i \cdot t^i$ has u zeros, we have

$$\begin{aligned} & |(p-1) \cdot Prob[< \alpha, s(x,y) >_p \equiv 0 \bmod p] - Prob[< \alpha, s(x,y) >_p \not\equiv 0 \bmod p]| \\ = & \left| (p-1) \cdot \frac{u \cdot p^m + (p^m - u) \cdot p^{m-1}}{p^{2m}} - \frac{(p^m - u) \cdot (p^m - p^{m-1})}{p^{2m}} \right| \\ = & \frac{(p-1) \cdot u}{p^m} \leq \frac{(p-1) \cdot (n-1)}{p^m} \end{aligned}$$

which gives the desired result. □

Corollary 4.2: Let $\epsilon > 0$ be given. Let p be a prime, and let n be a positive integer. Then, one can explicitly construct a sample space $S \subseteq \mathbb{Z}_p^n$ of size $|S| < p^4 \cdot n^2/\epsilon^2$ which is ϵ-biased with respect to MOD_p-tests.

Proof: Let m be the smallest positive integer such that $(p-1) \cdot (n-1)/p^m \leq \epsilon$. Then, by Proposition 4.1 the sample space S_m^n is ϵ-biased and satisfies $|S| = p^{2m}$, i.e., $|S| < p^4 \cdot n^2/\epsilon^2$. □

Indeed, if $n/p^{m-1} \approx \epsilon$, then $|S| \leq c \cdot p^2 n^2/\epsilon^2$ for some small constant $c > 0$.

Corollary 4.3: Let $\epsilon > 0$ be given. Let p be a prime, and let n be a positive integer. One can explicitly construct a sample space $S \subseteq \mathbb{Z}_p^n$ of size $|S| < 4 \cdot (1 - p^{-k})^2 \cdot p^2 \cdot n^2/\epsilon^2$ which is (ϵ, k)-independent.

Proof: Using Lemma 2.2 with $\epsilon := \epsilon \cdot p/(2 \cdot (1 - p^{-k}))$, the result follows with Corollary 4.2. □

Now, we consider the case of approximating nonuniform random variables.

Corollary 4.4: Let $\epsilon > 0$ be given. Let p be a prime, and let k, n be positive integers. Then one can explicitly construct a sample space $S \subseteq \mathbb{Z}_2^n$ of size $|S| < 2^{2k+2} \cdot (1 - p^{-k})^2 \cdot p^2 \cdot n^2/\epsilon^2$ which is (ϵ, k)-independent (with respect to the probability $1/p$), i.e., if $X = (x_1, x_2, \ldots, x_n)$ is chosen uniformly at random from S, then for any k positions $1 \leq i_1 < i_2 < \ldots < i_k \leq n$ and any sequence $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_k) \in \mathbb{Z}_2^k$ with z entries being 0 it holds that

$$\left| Prob[(x_{i_1}, x_{i_2}, \ldots, x_{i_k}) = (\alpha_1, \alpha_2, \ldots, \alpha_k)] - \frac{(p-1)^{k-z}}{p^k} \right| \leq \epsilon \; .$$

Proof: By Corollary 4.3, we can explicitly construct a sample space $S \subseteq \mathbb{Z}_p^n$ of size $|S| < 2^{2k+2} \cdot (1-p^{-k})^2 \cdot p^2 \cdot n^2/\epsilon^2$ which is $(\epsilon/2^k, k)$-independent. Then, by Theorem 3.2 the reduced space $\overline{S} \subseteq \mathbb{Z}_2^n$ (obtained from S by identifying all nonzero entries by 1) is (ϵ, k)-independent (with respect to the probability $1/p$). □

The sample spaces from above generate (ϵ, k)-independent random variables. Using as an additional tool parity check matrices of BCH-codes as in [ABI] and [NN], the size of S can be further reduced by replacing in the upper bounds for S for $p \geq 3$ the 'n' by '$k^2 \cdot \log_p n$', i.e., for example in Corollary 4.2 we obtain $|S| = O(p^4 k^4 (\log_p n)^2/\epsilon^2)$.

A simple application is the *heavy codeword problem* for linear codes over $\mathbb{Z}_p$. Let $M \in \mathbb{Z}_p^{m \times n}$ be an $n \times m$-matrix with no row containing only zero entries. One wants to find a vector $x \in \mathbb{Z}_p^n$ such that Mx has at least $\frac{p-1}{p} \cdot m$ nonzero entries. For a sample space $S \subseteq \mathbb{Z}_p^n$ which is ϵ-biased with respect to MOD_p-tests with $\epsilon < 1/m$, let $x \in S$ be chosen uniformly at random. For $i = 1, 2, \ldots, m$, let m_i be the ith row of matrix M. The weight $wt(x)$ of a vector is the number of nonzero entries of x. The expected value $E(wt(Mx))$ of the weight fulfills

$$\begin{aligned} E(wt(Mx)) &= \sum_{i=1}^{m} Prob[< m_i, x >_p \not\equiv 0 \bmod p] \\ &= \sum_{i=1}^{m} \frac{(p-1) - bias(< m_i, x >_p)}{p} \\ &\geq \frac{p-1}{p} \cdot m - \frac{\epsilon \cdot m}{p} . \end{aligned}$$

If $\epsilon < 1/m$, then $E(wt(Mx)) > \frac{p-1}{p} \cdot m - \frac{1}{p}$. As $wt(Mx)$ is an integer, there must be a codeword x such that the weight of Mx is at least $\lceil \frac{p-1}{p} \cdot m \rceil$. Thus, using exhaustive search the heavy codeword problem over $\mathbb{Z}_p$ is for $p = poly(n)$ in NC.

Another example comes from testing circuits, namely, in order to test circuits in which each gate depends on at most k inputs, one uses (n, k, p)-universal sets, cf. [NN], [NSS]. The elements are sequences taken from $\mathbb{Z}_p^n$, and for any set of k coordinates the projection on these contains all possible p^k sequences. If we have a k-wise δ-dependent sample space for $\delta < p^{-k}$, then this is also a (n, k, p)-universal set. The reason is simple. If for k coordinates $i_1, i_2, \ldots, i_k$, there is a sequence in the chosen sample space over $\mathbb{Z}_p^k$ which has probability 0, then the distance from the uniform distribution of $x_{i_1}, x_{i_2}, \ldots, x_{i_k}$ is at least $p^{-k} > \delta$. Using Theorem 2.5 and Corollary 4.2 together with the above mentioned BCH-codes, one can construct (n, k, p)-universal sets of size $O(\log n \cdot p^{3k+o(k)})$.

5 Discussion

Our considerations can be extended to the case where we have an arbitrary finite group instead of the group $\mathbb{Z}_p$ of residues modulo p, but the group should have no divisors of zero. If the group has divisors of zero, this can be handled by taking only the multiples of an element under consideration.

For approximating nonuniform distributions of identically distributed random variables we considered the case of $q = 1/p$ where p is a prime. The general case of q being an arbitrary rational number $0 \leq q \leq 1$ can be handled by choosing a prime p and an integer l such that $q \sim l/p$. Then, one uses linear tests where we do not distinguish whether a MOD_p-test gives the result zero or nonzero, but rather whether a MOD_p-test gives a result contained in the interval $\{0, 1, \ldots, l-1\}$ or in $\{l, l+1, \ldots, p-1\}$. The corresponding calculations are along the lines we discussed in this paper but are more technical. We only mention that instead of the functions Φ_β^c we use the functions $\Phi_\beta^{c,l} : \mathbb{Z}_p^n \to \mathrm{IR}$ with

$$\Phi_\beta^{c,l}(\alpha) = \begin{cases} -\frac{p-l}{\sqrt{p-1}} & \text{if } \sum_{i=1}^n \alpha_i\beta_i + c \equiv j \bmod p \text{ for some } j \in \{0, \ldots, l-1\} \\ \frac{l}{\sqrt{p-1}} & \text{else.} \end{cases}$$

6 Appendix

Lemma 2.2: Let $k \geq 1$ be a fixed positive integer. Let $S \subseteq \mathbb{Z}_p^n$ be a sample space which is ϵ-biased with respect to MOD$_p$-tests of size at most k. Then, the space S is $(2 \cdot \epsilon / p \cdot (1 - p^{-k}), k)$-independent.

Proof: Let $X = (x_1, x_2, \ldots, x_n)$ be chosen uniformly at random from the sample space S. By assumption, S is ϵ-biased with respect to MOD$_p$-tests of size at most k. Thus, for each element $c \in \mathbb{Z}_p$ and each sequence $\beta = (\beta_1, \beta_2, \ldots, \beta_n) \in \mathbb{Z}_p^n \setminus \{0^n\}$ with at most k nonzero entries, we have

$$|(p-1) \cdot \mathrm{Prob}[< \beta, X >_p + c \equiv 0 \bmod p] - \mathrm{Prob}[< \beta, X >_p + c \not\equiv 0 \bmod p]| \leq \epsilon \ . \qquad (13)$$

We consider w.l.o.g. the first k positions of X, i.e., $x_1, x_2, \ldots, x_k$. For each sequence $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_k) \in \mathbb{Z}_p^k$, let p_α denote the probability that $x_i = \alpha_i$ for $i = 1, 2, \ldots, k$. For $c \in \mathbb{Z}_p$ and $\beta \in \mathbb{Z}_p^k$, define

$$d_\beta^c = \sum_{\alpha \in \mathbb{Z}_p^k} \Phi_\beta^c(\alpha) \cdot p_\alpha \ . \qquad (14)$$

By definition of the functions Φ_β^c and using (13), we have

$$\begin{aligned} \left|d_\beta^c\right| &= \left| - \sum_{\alpha \in \mathbb{Z}_p^k; <\alpha,\beta>_p + c \equiv 0 \bmod p} p_\alpha \cdot \sqrt{p-1} + \sum_{\alpha \in \mathbb{Z}_p^k; <\alpha,\beta>_p + c \not\equiv 0 \bmod p} p_\alpha \cdot \frac{1}{\sqrt{p-1}} \right| \\ &= \frac{1}{\sqrt{p-1}} \cdot |(p-1) \cdot \mathrm{Prob}[< \beta, X >_p + c \equiv 0 \bmod p] - \mathrm{Prob}[< \beta, X >_p + c \not\equiv 0 \bmod p]| \\ &\leq \frac{\epsilon}{\sqrt{p-1}} \ . \qquad (15) \end{aligned}$$

Hence, d_β^c describes up to the factor $1/\sqrt{p-1}$ the absolute value of the *bias* of S with respect to the MOD$_p$-test given by c and β.

Claim 6.1: For every sequence $\gamma \in \mathbb{Z}_p^k$,

$$p_\gamma \ = \ p^{-(k+1)} \cdot \sum_{c \in \mathbb{Z}_p} \sum_{\beta \in \mathbb{Z}_p^k} d_\beta^c \cdot \Phi_\beta^c(\gamma) \ . \qquad (16)$$

Proof: Let the sequence $\gamma \in \mathbb{Z}_p^k$ be given. By multiplying (14) by $\Phi_\beta^c(\gamma)$ and summing over all possible values of $c \in \mathbb{Z}_p$ and $\beta \in \mathbb{Z}_p^k$, we obtain

$$\sum_{c\in\mathbb{Z}_p} \sum_{\beta\in\mathbb{Z}_p^k} d_\beta^c \cdot \Phi_\beta^c(\gamma) \quad = \quad \sum_{c\in\mathbb{Z}_p} \sum_{\beta\in\mathbb{Z}_p^k} \sum_{\alpha\in\mathbb{Z}_p^k} \Phi_\beta^c(\alpha) \cdot \Phi_\beta^c(\gamma) \cdot p_\alpha \; . \tag{17}$$

In the following, we will show that

$$\sum_{c\in\mathbb{Z}_p} \sum_{\beta\in\mathbb{Z}_p^k} \Phi_\beta^c(\gamma)^2 \cdot p_\gamma \quad = \quad p_\gamma \cdot p^{k+1} \tag{18}$$

and that

$$\sum_{c\in\mathbb{Z}_p} \sum_{\beta\in\mathbb{Z}_p^k} \sum_{\alpha\in\mathbb{Z}_p^k;\alpha\neq\gamma} \Phi_\beta^c(\alpha) \cdot \Phi_\beta^c(\gamma) \cdot p_\alpha = 0 \; . \tag{19}$$

To evaluate the right hand side of (17), consider

$$\sum_{c\in\mathbb{Z}_p} \sum_{\beta\in\mathbb{Z}_p^k} \Phi_\beta^c(\alpha) \cdot \Phi_\beta^c(\gamma) \cdot p_\alpha \tag{20}$$

for a fixed sequence $\alpha \in \mathbb{Z}_p^k$. We distinguish three cases according to the value of α; namely, Case 1: $\alpha = \gamma$, Case 2: α and γ are linearly independent, and Case 3: α and γ are linearly dependent. Let $\alpha \in \mathbb{Z}_p^k$ be fixed.

Case 1: Assume that $\alpha = \gamma$. Then, (20) becomes

$$\begin{aligned} \sum_{c\in\mathbb{Z}_p} \sum_{\beta\in\mathbb{Z}_p^k} \Phi_\beta^c(\gamma)^2 \cdot p_\gamma \quad &= \quad p_\gamma \cdot \sum_{\beta\in\mathbb{Z}_p^k} \left((-\sqrt{p-1})^2 + (p-1) \cdot \left(\frac{1}{\sqrt{p-1}} \right)^2 \right) \\ &= \quad p_\gamma \cdot p^{k+1} \; . \end{aligned} \tag{21}$$

Case 2: Next, we assume that α and γ are linearly independent. Let $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_k) \in \mathbb{Z}_p^k \setminus \{0^k\}$ and $\gamma = (\gamma_1, \gamma_2, \ldots, \gamma_k) \in \mathbb{Z}_p^k \setminus \{0^k\}$. Then, there are indices i, j with $1 \leq i < j \leq k$ such that the subsequences (α_i, α_j) and (γ_i, γ_j) are linearly independent in $\mathbb{Z}_p^2$. We want to count the number of terms $\Phi_\beta^c(\alpha) \cdot \Phi_\beta^c(\gamma)$ with the same value. To do so, for fixed $c \in \mathbb{Z}_p$, we partition the set $\mathbb{Z}_p^k$ into four sets, namely, $\mathbb{Z}_p^k = A_1(c) \uplus A_2(c) \uplus A_3(c) \uplus A_4(c)$ where

$$\begin{aligned} A_1(c) \quad &= \quad \left\{ \beta \in \mathbb{Z}_p^k \,|< \alpha, \beta >_p + c \equiv 0 \bmod p \text{ and } < \beta, \gamma >_p + c \equiv 0 \bmod p \right\} \\ A_2(c) \quad &= \quad \left\{ \beta \in \mathbb{Z}_p^k \,|< \alpha, \beta >_p + c \equiv 0 \bmod p \text{ and } < \beta, \gamma >_p + c \not\equiv 0 \bmod p \right\} \\ A_3(c) \quad &= \quad \left\{ \beta \in \mathbb{Z}_p^k \,|< \alpha, \beta >_p + c \not\equiv 0 \bmod p \text{ and } < \beta, \gamma >_p + c \equiv 0 \bmod p \right\} \\ A_4(c) \quad &= \quad \left\{ \beta \in \mathbb{Z}_p^k \,|< \alpha, \beta >_p + c \not\equiv 0 \bmod p \text{ and } < \beta, \gamma >_p + c \not\equiv 0 \bmod p \right\} \; . \end{aligned}$$

As (α_i, α_j) and (γ_i, γ_j) are linearly independent, these two vectors span $\mathbb{Z}_p^2$. Then, for any choice of $\beta_1, \ldots, \beta_{i-1}, \beta_{i+1}, \ldots, \beta_{j-1}, \beta_{j+1}, \ldots, \beta_k \in \mathbb{Z}_p$ and for any fixed $r_1, r_2 \in \mathbb{Z}_p$, there exist unique $\beta', \beta^* \in \mathbb{Z}_p$ such that $\beta = (\beta, \ldots, \beta_{i-1}, \beta', \beta_{i+1}, \ldots, \beta_{j-1}, \beta^*, \beta_{j+1}, \ldots, \beta_k)$

satisfies $< \alpha, \beta >_p + c \equiv r_1 \bmod p$ and $< \beta, \gamma >_p + c \equiv r_2 \bmod p$. Hence, the number of sequences $\beta \in \mathbb{Z}_p^k$ with $< \alpha, \beta >_p + c \equiv r_1 \bmod p$ and $< \beta, \gamma >_p + c \equiv r_2 \bmod p$ is equal to p^{k-2}. We infer that

$$\begin{aligned} |A_1(c)| &= p^{k-2} \\ |A_2(c)| = |A_3(c)| &= (p-1) \cdot p^{k-2} \\ |A_4(c)| &= (p-1)^2 \cdot p^{k-2} \,. \end{aligned}$$

Then, for fixed α, expression (20) becomes

$$\begin{aligned} & \sum_{c \in \mathbb{Z}_p} \sum_{\beta \in \mathbb{Z}_p^k} \Phi_\beta^c(\alpha) \cdot \Phi_\beta^c(\gamma) \cdot p_\alpha \\ = \;& p_\alpha \cdot \sum_{c \in \mathbb{Z}_p} \sum_{\beta \in A_1(c)} \sum_{\beta \in A_2(c)} \sum_{\beta \in A_3(c)} \sum_{\beta \in A_4(c)} \Phi_\beta^c(\alpha) \cdot \Phi_\beta^c(\gamma) \\ = \;& p_\alpha \cdot \sum_{c \in \mathbb{Z}_p} \left[|A_1(c)| \cdot (p-1) + 2 \cdot |A_2(c)| \cdot (-1) + |A_4(c)| \cdot \frac{1}{p-1} \right] \qquad (22) \\ = \;& 0 \,. \end{aligned}$$

Case 3: Finally, let α and γ be linearly dependent, but $\alpha \neq \gamma$. Then, we have $\alpha = l \cdot \gamma$ for some $l \in \mathbb{Z}_p \backslash \{1\}$. Assume first that $l \neq 0$ and $\gamma \neq 0^k$. We partition the set $\mathbb{Z}_p^k$ as in Case 2, namely for fixed $c \in \mathbb{Z}_p$ let $\mathbb{Z}_p^k = A_1(c) \uplus A_2(c) \uplus A_3(c) \uplus A_4(c)$. First, consider the set $A_1(c)$. If $\beta \in A_1(c)$, i.e., $< \alpha, \beta >_p + c \equiv < \beta, \gamma >_p + c \equiv 0 \bmod p$, then $(l-1) \cdot < \beta, \gamma >_p \equiv 0 \bmod p$. Since $l \neq 1$, we infer $< \beta, \gamma >_p \equiv 0 \bmod p$. As we assumed that $\gamma \neq 0^k$, we have

$$|A_1(c)| = \begin{cases} p^{k-1} & \text{if } c = 0 \\ 0 & \text{if } c \neq 0. \end{cases}$$

Next, we consider the set $A_2(c)$. Let $\beta \in A_2(c)$ and $c \neq 0$. If $< \alpha, \beta >_p + c \equiv 0 \bmod p$, we claim that $< \gamma, \beta >_p + c \not\equiv 0 \bmod p$. Namely, $< \gamma, \beta >_p + c \equiv \frac{1}{l} \cdot (< \alpha, \beta >_p + l \cdot c) \equiv \frac{1}{l} \cdot (-c + l \cdot c) \not\equiv 0 \bmod p$ as $l \neq 0, 1$ and p is a prime. Then, for $c \neq 0$, we only have to fulfill $< \alpha, \beta >_p + c \equiv 0 \bmod p$, and we have $|A_2(c)| = p^{k-1}$. For $c = 0$, however, we infer $< \alpha, \beta >_p \equiv 0 \bmod p$, i.e., $< \gamma, \beta >_p \equiv 0 \bmod p$, as $l \neq 0$. Thus, $|A_2(0)| = 0$, and by symmetry we have

$$|A_2(c)| = |A_3(c)| = \begin{cases} 0 & \text{if } c = 0 \\ p^{k-1} & \text{if } c \neq 0. \end{cases}$$

As $\mathbb{Z}_p^k = A_1(c) \uplus \ldots \uplus A_4(c)$, i.e., $\left|\mathbb{Z}_p^k\right| = \sum_{i=1}^4 |A_i(c)|$ for each $c \in \mathbb{Z}_p$, we infer $|A_4(c)| = p^k - \sum_{i=1}^3 |A_i(c)|$, hence

$$|A_4(c)| = \begin{cases} p^k - p^{k-1} & \text{if } c = 0 \\ p^k - 2p^{k-1} & \text{if } c \neq 0. \end{cases}$$

Then, (20) becomes

$$\sum_{c \in \mathbb{Z}_p} \sum_{\beta \in \mathbb{Z}_p^k} \Phi_\beta^c(\alpha) \cdot \Phi_\beta^c(\gamma) \cdot p_\alpha$$

$$\begin{aligned}
&= \sum_{i=1}^{4} \sum_{\beta\in A_i(0)} \Phi^0_\beta(\alpha)\cdot\Phi^0_\beta(\gamma)\cdot p_\alpha + \sum_{c\in\mathbb{Z}_p\setminus\{0\}} \sum_{i=1}^{4} \sum_{\beta\in A_i(c)} \Phi^c_\beta(\alpha)\cdot\Phi^c_\beta(\gamma)\cdot p_\alpha \\
&= p_\alpha\cdot\left[p^{k-1}\cdot\left(-\sqrt{p-1}\right)^2 + \left(p^k - p^{k-1}\right)\cdot\left(\frac{1}{\sqrt{p-1}}\right)^2\right] + \\
&\quad +p_\alpha\cdot\sum_{c\in\mathbb{Z}_p\setminus\{0\}}\left[2\cdot p^{k-1}\cdot(-1) + \left(p^k - 2\cdot p^{k-1}\right)\cdot\left(\frac{1}{\sqrt{p-1}}\right)^2\right] \qquad (23) \\
&= 0.
\end{aligned}$$

Now, let $\gamma = 0^k$ and $\alpha \neq 0^k$. We claim that

$$\sum_{c\in\mathbb{Z}_p}\sum_{\beta\in\mathbb{Z}_p^k} \Phi^c_\beta(\alpha)\cdot\Phi^c_\beta(\gamma)\cdot p_\alpha = 0\ . \tag{24}$$

Namely,

$$\begin{aligned}
&\sum_{c\in\mathbb{Z}_p}\sum_{\beta\in\mathbb{Z}_p^k} \Phi^c_\beta(\alpha)\cdot\Phi^c_\beta(\gamma)\cdot p_\alpha \\
&= p_\alpha\cdot\sum_{\beta\in\mathbb{Z}_p^k}\Phi^0_\beta(\alpha)\cdot(-\sqrt{p-1}) + p_\alpha\cdot\sum_{c\in\mathbb{Z}_p\setminus\{0\}}\sum_{\beta\in\mathbb{Z}_p^k}\Phi^c_\beta(\alpha)\cdot\frac{1}{\sqrt{p-1}} \\
&= p_\alpha\cdot(p^{k-1}\cdot(-\sqrt{p-1})^2 + (p^k - p^{k-1})\cdot(-1)) + \\
&\quad +p_\alpha\cdot\left((p-1)\cdot p^{k-1}\cdot(-\sqrt{p-1})\cdot\frac{1}{\sqrt{p-1}} + (p-1)\cdot(p^k - p^{k-1})\cdot\frac{1}{(\sqrt{p-1})^2}\right) \\
&= 0\ .
\end{aligned}$$

Summarizing (18), (19) and (17), we proved equality (16), and hence Claim 6.1.

□

We continue with the proof of Lemma 2.2. By (16), we have for fixed $\gamma\in\mathbb{Z}_p^k$ that

$$p_\gamma - p^{-k-1}\cdot\sum_{c\in\mathbb{Z}_p} d^c_{0^k}\cdot\Phi^c_{0^k}(\gamma) \quad = \quad p^{-k-1}\cdot\sum_{c\in\mathbb{Z}_p}\sum_{\beta\in\mathbb{Z}_p^k\setminus\{0^k\}} d^c_\beta\cdot\Phi^c_\beta(\gamma). \tag{25}$$

Although we know only approximate values for the probabilities of the occurring subsequences, the identity $\sum_{\alpha\in\mathbb{Z}_p^k} p_\alpha = 1$ holds in any case. Using this, we obtain

$$\begin{aligned}
&p^{-k-1}\cdot\sum_{c\in\mathbb{Z}_p} d^c_{0^k}\cdot\Phi^c_{0^k}(\gamma) = p^{-k-1}\cdot\left(d^0_{0^k}\cdot\phi^0_{0^k}(\gamma) + \sum_{c\in\mathbb{Z}_p\setminus\{0\}} d^c_{0^k}\cdot\Phi^c_{0^k}(\gamma)\right) \\
&= p^{-k-1}\cdot\left(d^0_{0^k}\cdot(-\sqrt{p-1}) + \frac{1}{\sqrt{p-1}}\cdot\sum_{c\in\mathbb{Z}_p\setminus\{0\}} d^c_{0^k}\right) \\
&= p^{-k-1}\cdot\left((-\sqrt{p-1})\cdot\sum_{\alpha\in\mathbb{Z}_p^k}\Phi^0_{0^k}(\alpha)\cdot p_\alpha + \frac{1}{\sqrt{p-1}}\cdot\sum_{c\in\mathbb{Z}_p\setminus\{0\}}\sum_{\alpha\in\mathbb{Z}_p^k}\Phi^c_{0^k}(\alpha)\cdot p_\alpha\right)
\end{aligned}$$

$$\begin{aligned} &= p^{-k-1} \cdot \left((p-1) \cdot \sum_{\alpha \in \mathbb{Z}_p^k} p_\alpha + \frac{1}{p-1} \cdot \sum_{c \in \mathbb{Z}_p \setminus \{0\}} \sum_{\alpha \in \mathbb{Z}_p^k} p_\alpha \right) \\ &= p^{-k} \, . \end{aligned}$$

With (25), we infer

$$|p_\gamma - p^{-k}| = p^{-k-1} \cdot \left| \sum_{c \in \mathbb{Z}_p} \sum_{\beta \in \mathbb{Z}_p^k \setminus \{0^k\}} d_\beta^c \cdot \Phi_\beta^c(\gamma) \right| \, . \tag{26}$$

By (15), i.e., $|d_\beta^c| \leq \epsilon / \sqrt{p-1}$, we conclude

$$\begin{aligned} & |p_\gamma - p^{-k}| \leq p^{-k-1} \cdot \sum_{c \in \mathbb{Z}_p} \sum_{\beta \in \mathbb{Z}_p^k \setminus \{0^k\}} \left| d_\beta^c \right| \cdot \left| \Phi_\beta^c(\gamma) \right| \\ \leq \; & p^{-k-1} \cdot \frac{\epsilon}{\sqrt{p-1}} \cdot \sum_{\beta \in \mathbb{Z}_p^k \setminus \{0^k\}} \sum_{c \in \mathbb{Z}_p} |\Phi_\beta^c(\gamma)| = p^{-k-1} \cdot \frac{\epsilon}{\sqrt{p-1}} \cdot \sum_{\beta \in \mathbb{Z}_p^k \setminus \{0^k\}} \left(\sqrt{p-1} + \frac{p-1}{\sqrt{p-1}} \right) \\ = \; & \frac{2 \cdot \epsilon}{p} \cdot \left(1 - p^{-k} \right) \end{aligned}$$

which finishes the proof of Lemma 2.2. □

References

[ABI] N. Alon, L. Babai and A. Itai, *A Fast and Simple Randomized Parallel Algorithm for the Maximal Independent Set Problem,* Journal of Algorithms 7, 1985, 567-583.

[ABNR] N. Alon, J. Bruck, J. Naor, M. Naor and R. Roth, *Construction of Asymptotically Good Low-Rate Error-Correcting Codes Through Pseudo-Random Graphs,* IEEE Transactions on Information Theory 38, 1992, 509-516.

[AGHP] N. Alon, O. Goldreich, J. Håstad and R. Peralta, *Simple Constructions of Almost k-wise Independent Random Variables,* Random Structures & Algorithms 3, 1992, 289-304. Addendum: Random Structures & Algorithms 4, 1993, 119-120.

[AS] N. Alon and J. Spencer, *The Probabilistic Method,* Wiley & Sons, New York, 1992.

[AMN] Y. Azar, R. Motwani and J. Naor, *Approximating Probability Distributions Using Small Sample Spaces,* preprint, 1995.

[BFS] L. Babai, P. Frankl and J. Simon, *Complexity Classes in Communication Complexity Theory,* Proceedings 27th Annual IEEE Symposium on Foundations of Computer Science FOCS'86, 1986, 337-347.

[BC] J. Beck and W. Chen, *Irregularities of Distribution,* Cambridge University Press, 1987.

[BR] B. Berger and J. Rompel, *Simulating* $(\log n)^c$*-wise Independence in NC,* Journal of the ACM 38, 1991, 1026-1046.

[Be] C. Bertram-Kretzberg, *TH-MOD_p-circuits,* preprint, 1997.

[CRS] S. Chari, P. Rohatgi and A. Srinivasan, *Improved Algorithms via Approximations of Probability Distributions,* Proc. 26th Annual Symposium on the Theory of Computing STOC'96, 1996, 584-592.

[CG] B. Chor and O. Goldreich, *On the Power of Two-point Based Sampling,* Journal of Complexity 5, 1989, 96-106.

[CGW] F. R. K. Chung, R. L. Graham and R. M. Wilson, *Quasi-Random Graphs,* Combinatorica 9, 1989, 345-362.

[Ev] G. Even, *Construction of Small Probability Spaces for Deterministic Simulation,* M. Sc. thesis, Technion, Haifa, Israel, 1991.

[EGLNV] G. Even, O. Goldreich, M. Luby, N. Nisan and B. Velicković, *Approximations of General Independent Distributions,* Proc. 24th Annual ACM Symposium on the Theory of Computing STOC'92, 1992, 10-16.

[HPS] J. Håstad, S. Phillips and S. Safra, *A Well Characterized Approximation Problem,* Information Processing Letters 47, 1993, 301-305.

[KM] H. Karloff and Y. Mansour, *On Construction of k-wise Independent Random Variables,* Proc. 24th Annual Symposium on the Theory of Computing STOC'94, 1994, 564-573.

[KW] R. M. Karp and A. Wigderson, *A Fast Parallel Algorithm for the Maximal Independent Set Problem,* Journal of the ACM 32, 1985, 762-773.

[KP] M. Krause and P. Pudlak, *On the Computational Power of Depth* 2 *Circuits with Threshold Modulo Gates,* Proc. 26th Annual ACM Symposium on the Theory of Computing STOC'94, 1994, 48-57.

[LPS] A. Lubotzky, R. Phillips and P. Sarnak, *Ramanujan Graphs,* Combinatorica 8, 1988, 261-277.

[Lu] M. Luby, *Removing Randomness in Parallel Computation without a Processor Penalty,* Proc. 29th Annual Symposium on Foundations of Computer Science, 1988, 162-173.

[MNN] R. Motwani, J. Naor and M. Naor, *The Probabilistic Method Yields Deterministic Parallel Algorithms,* Journal of Computer and System Sciences 49, 1994, 478-516.

[NN] J. Naor and M. Naor, *Small Bias Probability Spaces: Efficient Constructions and Applications,* SIAM Journal on Computing 22, 1993, 838-856.

[NSS] M. Naor, L. J. Schulman and A. Srinivasan, *Splitters and Near-Optimal Derandomization,* Proc. 36th Annual Symp. on Foundations of Computer Science, 1995, 182-191.

[Pe] R. Peralta, *On the Randomness Complexity of Algorithms,* CS Research Report TR 90-1, University of Wiskonsin, Milwaukee, 1990.

[Va] U. Vazirani, *Randomness, Adversaries and Computation,* PhD thesis, University of California, Berkeley, 1986.