J. Phys. A: Math. Gen. **31** (1998) 3731–3749. Printed in the UK PII: S0305-4470(98)85983-0

On the ground states of the Bernasconi model

Stephan Mertens† and Christine Bessenrodt‡

† Institut für Theoretische Physik, Otto-von-Guericke Universität, Postfach 4120, D-39016 Magdeburg, Germany

‡ Institut für Algebra und Geometrie, Otto-von-Guericke Universität, Postfach 4120, D-39016 Magdeburg, Germany

Received 15 July 1997

Abstract. The ground states of the Bernasconi model are binary ± 1 sequences of length N with low autocorrelations. We introduce the notion of perfect sequences, binary sequences with one-valued off-peak correlations of minimum amount. If they exist, they are ground states. Using results from the mathematical theory of cyclic difference sets, we specify all values of N for which perfect sequences exist and how to construct them. For other values of N, we investigate almost perfect sequences, i.e. sequences with two-valued off-peak correlations of minimum amount. Numerical and analytical results support the conjecture that almost perfect sequences exist for all values of N, but that they are not always ground states. We present a construction for low-energy configurations that works if N is the product of two odd primes.

1. Introduction

Binary sequences of $+1$ and -1 with low autocorrelations have many applications in communication engineering [1]. Their construction has a long history [2], and has turned out to be a very hard mathematical problem. Bernasconi [3] introduced an Ising spin model that allows us to formulate the construction problem in the framework of statistical mechanics.

Consider a sequence of binary variables or Ising spins of length N,

$$S = (s_0, s_1, \ldots, s_{N-1}) \qquad s_i = \pm 1 \tag{1}$$

and their autocorrelations

$$C_g(S) = \sum_{i=0}^{N-1} s_i s_{i+g} \tag{2}$$

where all indices are taken modulo N. Bernasconi defined a Hamiltonian $H(S)$ by

$$\begin{aligned} H(S) &= \sum_{g=1}^{N-1} C_g^2(S) \\ &= \sum_{i,j=0}^{N-1} \sum_{g=1}^{N-1} s_i s_{i+g} s_j s_{j+g}. \end{aligned} \tag{3}$$

The ground states of this model with its long-range, four-spin interactions are the low-autocorrelation binary sequences we are looking for.

The Bernasconi model is completely deterministic in the sense that there is no explicit or quenched disorder like in spin-glasses. Nevertheless the ground states are by definition

0305-4470/98/163731+19$19.50

highly disordered. This self-induced disorder resembles the situation in real glasses. In fact, the Bernasconi model exhibits features of a glass transition like a jump in the specific heat [3], and slow dynamics and aging [4].

The replica scheme, an analytical method well established in spin-glass theory, is of little use for deterministic systems. People have approximated the Bernasconi model by a model with explicit, quenched disorder, which in turn can be analysed analytically with the replica method [5, 6]. This approach is only valid in the high-temperature regime, however, and provides only estimates for the ground-state energies.

Bernasconi introduced his model in order to apply statistical mechanics, especially simulated annealing, to find low-autocorrelation binary sequences. His approach turned out to be of little practical use, however: the energy minima found with the annealing procedure differ by a factor of 2 from the conjectured ground-state energy. This failure is due to the peculiar 'golf course' property of the energy landscape which is dominated by a large number of local minima, while the global minima are deep and shallow holes, extremely isolated in configurations space.

The original Bernasconi model is defined with aperiodic autocorrelations, i.e. with $N-1-g$ as the upper summation limit in equation (2). For this model, exhaustive enumeration of all 2^N configurations seems to be the only means of obtaining true ground states [7, 8].

For the Bernasconi model with periodic autocorrelations, the situation is better. The tight connection between the correlations of periodic binary sequences and mathematical objects called *cyclic difference sets* can be exploited to obtain some exact results on the ground states. The theory of difference sets is well established in mathematics but hardly known in statistical mechanics. It is one objective of this paper to fill this gap. It will turn out that ground states of the Bernasconi model can be constructed from cyclic difference sets for certain values of N. Other values of N require some generalizations. Guided by numerical results, we will discuss such generalizations.

This paper is organized as follows. We start with a derivation of the equivalence of autocorrelations in binary sequences and cyclic difference sets in section 2. In section 3, we introduce *perfect sequences*, which are ground states of the Bernasconi model—if they exist. The existence problem in turn can be answered using results from the theory of difference sets. Numerical and analytical investigations of those cases, which are not covered by perfect sequences, can be found in section 4. Section 5 comprises our conclusions.

2. Difference sets

Let $G = \mathbb{Z}_N$, the *cyclic group* of integers $0, \ldots, N-1$ with addition modulo N, and let $D \subseteq G$ be a k-element subset of G. Each element $g \in G$ has a number of different representations $g = d_1 - d_2$ with $d_1, d_2 \in D$, denoted as *replication number* $\lambda(g)$:

$$\lambda(g) = |\{(d_1, d_2) | g = d_1 - d_2, d_1, d_2 \in D\}|. \tag{4}$$

The trivial case is $\lambda(0) = k$. The values $\lambda(g)$ for $g \neq 0$ depend on D. The total number of differences $d_1 - d_2$ equals k^2, leading to the constraint

$$k^2 = \sum_{g \in G} \lambda(g). \tag{5}$$

Now consider the periodic binary sequence (s_i) associated with D:

$$_i = \begin{cases} +1 & i \bmod N \in D \\ -1 & i \bmod N \notin D. \end{cases} \tag{6}$$

A straightforward calculation shows that the autocorrelations of this sequence are given by

$$C_g = N - 4(k - \lambda(g)). \tag{7}$$

The converse is also true: given a ± 1 sequence of length N with periodic autocorrelations $C(g)$, each $g \in G$ has $\lambda(g) = k + (C(g) - N)/4$ representations $g = d_1 - d_2$ within the k-element set

$$D := \{i : s_i = +1, i = 0, \ldots, N-1\} \tag{8}$$

so we conclude that the periodic autocorrelations of a binary sequence and the number of difference representations of elements of a cyclic group G in $D \times D$ are equivalent.

The definition of a replication number and its correspondence to the correlations of periodic binary sequences do not depend on the concrete realization of our group G as $G = \mathbb{Z}_N$. Let G be a cyclic group of order N, written in multiplicative notation. The replication number $\lambda(g)$ is defined as

$$\lambda(g) = |\{(d_1, d_2) | g = d_1 \cdot d_2^{-1}, d_1, d_2 \in D\}| \tag{9}$$

for a k-element subset $D \subseteq G$. To construct a periodic binary sequence based on D, we choose a generator α of the cyclic group G and define the binary sequence to be

$$s_i = \begin{cases} +1 & \alpha^i \in D \\ -1 & \alpha^i \notin D. \end{cases} \tag{10}$$

Again the correlations of this sequence are given by equation (7).

If the replication number is constant for $g \neq 0$, i.e.

$$\lambda(g) = \begin{cases} k & \text{for } g = 0 \\ \lambda & \text{for } g \neq 0 \end{cases} \tag{11}$$

the set D is called an (N, k, λ) *cyclic difference set*, where the term cyclic refers to the fact that the underlying group G is cyclic—obvious variants are general or Abelian difference sets. $D = \{1, 2, 4\} \subset \mathbb{Z}_7$ is an example of a $(7, 3, 1)$ cyclic difference set.

Difference sets have been studied by mathematicians for more than half a century, see [9–11] for a survey. They prove useful in various fields such as finite geometry or design theory. According to equation (7) it is obvious that cyclic difference sets and binary sequences with *constant off-peak autocorrelations* are essentially the same objects.

The fundamental questions in the field of difference sets concern their *existence* and their *construction*. Albeit being unsolved in general, the existence question can be answered for special sets of parameters (N, k, λ). Most of the results are non-existence theorems which impose necessary conditions on (N, k, λ) for a cyclic difference set to exist [9]. A simple non-existence theorem is given by equation (5), which for a (general) difference set reads

$$k(k-1) = \lambda(N-1). \tag{12}$$

See [9] for other, more sophisticated non-existence theorems. All known existence proofs are constructive, i.e. they provide an explicit method to construct a cyclic difference set.

Table 1. Classes of N which allow the construction of a Hadamard difference set resp. a perfect binary sequence with all off-peak correlations $C_g = -1$.

$N = 2^j - 1,\ j \geqslant 2$	m-sequence
$N = 4t + 3$ prime	Legendre sequence
$N = p(p+2)$ $p, p+2$ prime	twin-prime sequence

3. Perfect sequences

We define a *perfect sequence* to be a binary sequence with one-valued off-peak autocorrelations of minimum amount, i.e. with

$$C_{g\neq 0} = \begin{cases} 0 & N \equiv 0 \bmod 4 \\ 1 & N \equiv 1 \bmod 4 \\ 2 & N \equiv 2 \bmod 4 \\ -1 & N \equiv 3 \bmod 4. \end{cases} \tag{13}$$

Equation (12) excludes the existence of perfect sequences with all $C_{k>0} = -2$ for $N = 4t - 2 > 2$.

Obviously any perfect sequence is a ground state of the Bernasconi model. To find perfect sequences, we have to look for cyclic difference sets with parameters

$$k - \lambda = t \qquad N = 4t, 4t \pm 1, 4t - 2. \tag{14}$$

3.1. Hadamard difference sets

Let us first consider the case $N \equiv 3 \bmod 4$. According to equation (12), the cyclic difference set that corresponds to a perfect sequence must have parameters of the form

$$(N, k, \lambda) = (4t - 1, 2t - 1, t - 1) \tag{15}$$

for some integer $t > 0$. Such difference sets are called *Hadamard difference sets*. All *known* Hadamard difference sets can be classified into three classes according to the value of N (table 1). In fact it has been shown that all Hadamard difference sets with $N \leqslant 10\,000$ belong to one of the above parameter classes, with 17 possible exceptions (all of them > 1000) [12]. This result has been accomplished by the extensive use of non-existence theorems. A physicist may conclude that there are no Hadamard difference sets for other parameters. The three classes cover 195 out of 250 values $N = 4t + 3 < 1000$. Table 1 lists a construction rule for every parameter class. Beside these rules, there are additional construction methods which lead to non-equivalent Hadamard difference sets for some parameter such as $N = 4t + 3 = 4x^2 + 27$, N prime, for integer x [9].

We start with the description of m-sequences. Let p be a prime and $F = \mathrm{GF}(p)$ be the finite field of order p. A *shift register sequence* produced by a *linear feedback shift register* (LFSR) of order n over F is a sequence $\boldsymbol{a} = (a_k)$ of elements from F that satisfies the linear recurrence relation

$$a_i = \sum_{j=1}^{n} c_j a_{i-j} \qquad i \geqslant n. \tag{16}$$

The sequence is uniquely determined by the initial conditions $(a_0, \ldots, a_{n-1})$ and the feedback coefficients $(c_1, \ldots, c_n)$, $c_j \in F$. The name 'shift register sequence' stems from a hardware realization of equation (16).

There are p^n distinct n-tuples over F. The **0** tupel $(0, \ldots, 0)$ reproduces itself under the linear recurrence relation. Therefore a LFSR of order n over GF(p) produces a sequence which is ultimately periodic with period $\leqslant p^n - 1$. A sequence with least period $p^n - 1$ is called a maximum period sequence or, for short, an m-sequence.

Note that in an m-sequence each n-tupel except **0** occurs exactly once. Hence, an m-sequence is independent of the initial conditions and solely determined by the recursion coefficients $\boldsymbol{c}$. A well known theorem [13, ch 6] states that a LFSR with coefficients $(c_1, \ldots, c_n)$ produces an m-sequence if and only if the associated feedback polynomial

$$f(x) = 1 - c_1 x - c_2 x^2 - \cdots - c_n x^n \tag{17}$$

is a primitive polynomial. Primitive polynomials of all degrees exist for finite fields of any order p, i.e. for every prime p there is an LFSR of length n that produces a sequence of period $p^n - 1$, the maximum value.

Supplied with an m-sequence over $F = \mathrm{GF}(2)$, we can define a binary sequence via

$$s_i = (-1)^{a_i} = (-1)^{c_1 a_{i-1} + \cdots + c_n a_{i-n}}. \tag{18}$$

This sequence then satisfies the multiplicative recursion

$$s_i = s_{i-1}^{c_1} \cdot s_{i-2}^{c_2} \ldots s_{i-n}^{c_n} \tag{19}$$

which produces an m-sequence, meaning that every n-tupel of ± 1-values except the all-1 tupel $(1, 1, \ldots, 1)$ occurs exactly once as a subsequence $(s_t, s_{t+1}, \ldots, s_{t+n-1})$ in (s_i). It is easy to see that the product sequence $d_i = s_i s_{i+g}$ has the same recursion as the s_i

$$d_i = d_{i-1}^{c_1} \cdot d_{i-2}^{c_2} \ldots d_{i-n}^{c_n}. \tag{20}$$

Since (s_i) is an m-sequence, (d_i) equals (s_i) (for $g \neq 0$) except for a possible shift in the index,

$$d_i = s_{i+s} \tag{21}$$

for some s. Using this result, we find for the correlations of the sequence $S = (s_0, \ldots, s_{N-1})$, $N = 2^n - 1$,

$$C_g = \sum_{i=0}^{2^n-2} s_{i+s} = \sum_{i=0}^{2^n-2} s_i = -1 \tag{22}$$

since exactly 2^{n-1} of the s_i equal -1 and the remaining $2^{n-1} - 1$ equal $+1$.

As we have seen, m-sequences over GF(2) with period $2^n - 1$ can be used to construct perfect binary sequences with the same period. This construction requires a primitive polynomial of order n over GF(2). Tables of such polynomials can be found in the literature [14–16].

Now we discuss the construction of *Legendre sequences*. Let p be an odd prime. Exactly half of the elements $g \in \mathrm{GF}(p)^* = \mathrm{GF}(p) \setminus \{0\}$ are *squares*, i.e. they have a representation $g \equiv x^2 \bmod p$ with $x \in \mathrm{GF}(p)^*$. The other half cannot be written as a square. A convenient notation for this property is the *quadratic character*

$$\chi_p(g) = \begin{cases} 0 & g = 0 \\ 1 & g \text{ is a square in } \mathrm{GF}(p)^* \\ -1 & \text{otherwise.} \end{cases} \tag{23}$$

The quadratic character can easily be calculated using Euler's criterion [1, ch 15]:

$$\chi_p(g) = g^{\frac{1}{2}(p-1)} \bmod p \tag{24}$$

and it obeys

$$\sum_{x\in \mathrm{GF}(p)} \chi_p(x)\chi_p(x+g) = -1 \tag{25}$$

for all $g \neq 0$. This *orthogonality* of χ_p translates into good correlation properties of the so-called *Legendre sequence* of length p

$$s_i = \begin{cases} 1 & i \equiv 0 \bmod p \\ \chi_p(i) & \text{otherwise.} \end{cases} \tag{26}$$

The periodic off-peak autocorrelations of the Legendre sequence read

$$\begin{aligned} C_g &= \sum_{i=0}^{p-1} s_i s_{i+g} \\ &= \chi_p(g) + \chi_p(-g) + \sum_{i=0}^{p-1} \chi_p(i)\chi_p(i+g) \\ &= \chi_p(g)(1 + (-1)^{(p-1)/2}) - 1 \end{aligned}$$

i.e.

$$C_g = \begin{cases} -1 & p \equiv 3 \bmod 4 \\ +1, -3 & p \equiv 1 \bmod 4. \end{cases} \tag{27}$$

For $p \equiv 3 \bmod 4$ the Legendre sequence corresponds to a cyclic Hadamard difference set. For $p \equiv 1 \bmod 4$ exactly half of the autocorrelations take on the value $+1$, the other half takes on the value -3.

The discrete Fourier transform (DFT),

$$B_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \mathrm{e}^{-\mathrm{i}2\pi kj/N} s_j \tag{28}$$

of a Legendre sequence is given by [1, ch 15]

$$B_k = \begin{cases} \dfrac{1}{\sqrt{p}} - \mathrm{i}s_k & m \not\equiv 0 \bmod p \\ \dfrac{1}{\sqrt{p}} & m \equiv 0 \bmod p \end{cases} \tag{29}$$

for $p \equiv 3 \bmod 4$. This peculiar similarity between the Legendre sequence and its DFT, $\mathrm{Im}\, B_k = -s_k$ ($k \not\equiv 0 \bmod p$), turns the Legendre sequences into ground states of another deterministic model with glassy properties,

$$\begin{aligned} \tilde{H} &= \sum_{k=1}^{p-1} |s_k + \mathrm{Im}\, B_k|^2 \\ &= \sum_{k=1}^{p-1} |s_k - \frac{1}{\sqrt{p}} \sum_{j=0}^{p-1} \sin(2\pi jk/p) s_j|^2 \end{aligned} \tag{30}$$

the so-called sine-model [17].

The last entry in table 1 refers to the *twin-prime sequences*. Let p, q be odd primes with $p > q$. Consider the binary sequence of length pq,

$$s_i = \begin{cases} +1 & i \equiv 0 \bmod p \\ -1 & i \equiv 0 \bmod q,\ i \not\equiv 0 \bmod p \\ \chi_p(i)\chi_q(i) & \text{otherwise.} \end{cases} \tag{31}$$

If p and q are twin primes ($p = q + 2$), all correlations of this sequence equal -1. A proof will be given in section 4, where we discuss the case of general odd prime numbers p and q.

3.2. Menon difference sets

Now we consider the case $N \equiv 0 \bmod 4$. Equation (12) enforces

$$(N, k, \lambda) = (4u^2, 2u^2 - u, u^2 - u) \tag{32}$$

for some integer $u > 0$ for the cyclic difference set that corresponds to a perfect sequence. A cyclic difference set that satisfies equation (32) is called a *Menon difference set*. The corresponding binary sequence forms the row of a circulant Hadamard† matrix. For example $u = 1$, written as binary sequence:

$$(s) = (+1, +1, +1, -1). \tag{33}$$

Unfortunately, this is the only known example of a Menon difference set. In fact, it has been shown [18] that no Menon difference set exists for $1 < u < 250$ with the possible exceptions $u = 165$ and $u = 231$. There is a tight connection between Menon difference sets and *Barker sequences*, i.e. binary sequences with

$$\left| \sum_{i=0}^{N-1-g} s_i s_{i+g} \right| \leqslant 1. \tag{34}$$

The existence of a Barker sequence of even length N implies the existence of a Menon difference set of order N [19, 20]. It is not known whether the converse is also true. It has been shown, however, that there are no Barker sequences for $13 < N < 2.5 \times 10^9$ with the possible exception $N = 1596\,961\,444$ [18]. Therefore, it is still an unproven, but widely accepted conjecture, that no Menon difference set exists for $N > 4$.

3.3. Other difference sets

Another family of cyclic difference sets can be constructed for parameters

$$(N, k, \lambda) = \left(\frac{q^{\nu+1} - 1}{q - 1}, \frac{q^{\nu} - 1}{q - 1}, \frac{q^{\nu-1} - 1}{q - 1} \right) \tag{35}$$

where $\nu \leqslant 1$ and q is a prime power. Such sets are called *Singer difference sets* [9].

For $q = 2$ we rediscover the parameters of the Hadamard difference sets based on m-sequences, $q = 3$, $\nu = 1$ corresponds to the lonely Menon difference set (33). The only other cases where Singer difference sets yield ground states of the Bernasconi model are

q	ν	(N, k, λ)	$C_{g\neq 0}$
4	1	(5, 1, 0)	1
5	1	(6, 1, 0)	2
3	2	(13, 4, 1)	1.

Since the Singer difference sets yield ground states for only three new values of N, we will not discuss their construction.

According to equation (12), a difference set with $N \equiv 1 \bmod 4$ and $C_g = 1$ must have parameters of the form

$$(N, k, \lambda) = (2u(u + 1) + 1, u^2, \tfrac{1}{2}u(u - 1)) \tag{36}$$

† This is the reason why Menon difference sets are sometimes called Hadamard difference sets in the mathematical literature. Our Hadamard difference sets are then called Paley–Hadamard difference sets [13, p 232].

for some integer $u > 0$. It has been shown [21] that no such cyclic difference set exists for $3 \leqslant u \leqslant 100$, i.e. $13 < N \leqslant 20\,201$, so again it is well founded to believe that beyond $N = 13$ there are no such sets at all.

For $N = 4t - 2$, sequences with all $C_{k>0} = 2$ require

$$3t = u^2 + 2 \tag{37}$$

with integer u, i.e. $N = 2, 6, 22, 26, 66, \ldots$. Except for $N = 2$ and $N = 6$, no such sequences are known.

Other difference sets exist, but either their parameters coincide with one of the sets already discussed, or they lead to values for the off-peak autocorrelations that are far from a ground state.

4. Beyond perfect sequences

In the preceding section we have seen that for many values of N perfect sequences do not exist. In this section we introduce a generalization called *almost perfect sequences* and discuss their appearance as ground states of the Bernasconi model. In addition, we present a construction method for $N = pq$, p and q odd primes, that yields configurations with low energies, and we discuss generalized *Jacobi sequences*.

4.1. Almost perfect sequences

An almost perfect sequence is a binary sequence with two-valued off-peak autocorrelations of minimum amount, i.e. with

$$C_{g\neq 0} \in \begin{cases} \{0, \pm 4\} & N \equiv 0 \bmod 4 \\ \{1, -3\} & N \equiv 1 \bmod 4 \\ \{-2, 2\} & N \equiv 2 \bmod 4 \\ \{-1, 3\} & N \equiv 3 \bmod 4. \end{cases} \tag{38}$$

Again we have an ambiguity: for $N \equiv 0 \bmod 4$ all correlations are either $\in \{0, +4\}$ or $\in \{0, -4\}$. A sequence with three-valued correlations $C_g \in \{-4, 0, +4\}$ does not match our definition.

An almost perfect sequence corresponds to a set D with a two-valued replication number where the two replication numbers differ by one:

$$\lambda(g) = \begin{cases} k & g = 0 \\ \lambda + 1 & g \in U \subset G \\ \lambda & g \notin U. \end{cases} \tag{39}$$

U can be any subset of the underlying cyclic group G. We call a set D with such replication number an *almost cyclic difference set*.

Values of N that allow the construction of perfect sequences are rare, as we have seen in the preceding section. The question is whether the weaker constraint of almost perfectness can be fulfilled for more values of N.

To study this question we counted all almost perfect sequences of given length N by exhaustive enumeration (figure 1). Their number seems to increase exponentially with N but much slower than 2^N. From figure 1 we may conclude that there are almost perfect sequences for *all* values of N but their relative volume in configuration space decreases exponentially with N.

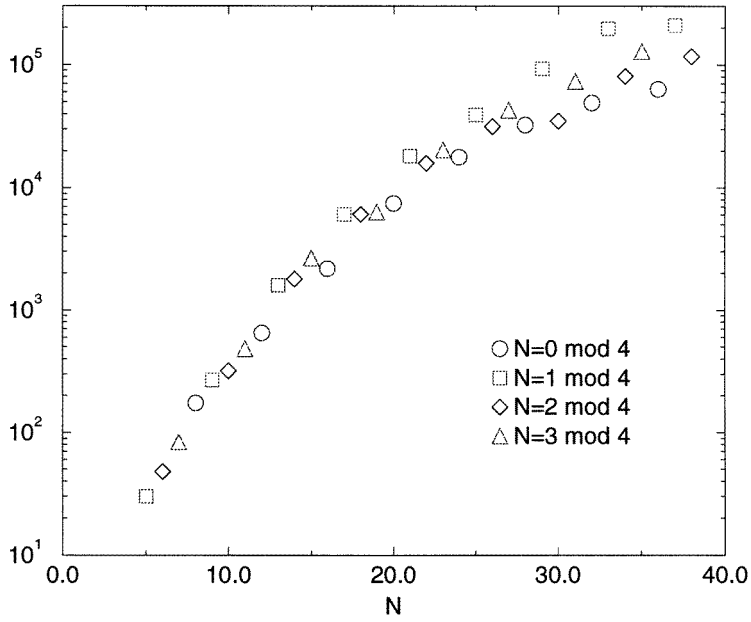

Figure 1. Total number of almost perfect binary sequences.

For larger values of N, this conclusion is supported by a heuristic numerical search. We start with a random sequence and lower its energy by single spin-flips until we obtain a sequence whose energy can no longer be lowered by flipping a single spin. If this local minimum is an almost perfect sequence, the procedure stops. If not, it starts again with a new random configuration.

With this algorithm we found almost perfect sequences for all $N < 84$. The CPU time increased strongly with N, so we stopped the search for larger values of N before an almost perfect sequence had been found. Random search is of course not well suited for configurations that are very rare. As an example, consider this: nine workstations searched the configuration space for $N = 86$ in parallel to find a sequence with $C_g = \pm 2$. After 20 days, two machines have found sequences with all $C_g = \pm 2$ for all $g > 0$ except $C_{43} = 6$, while the other seven machines still report sequences with at least two correlations $C_g = 6$ as their best results. The failure of random search for large values of N does not indicate the non-existence of almost perfect sequences.

Compared with difference sets, much less is known about the construction of almost difference sets. We only know two construction methods for almost perfect sequences: Legendre sequences for $N = 4t + 1$ prime (see section 3) and a construction due to Lempel *et al* [22] for $N = p^m - 1$ where p is an odd prime and m is a positive integer.

The construction of Lempel *et al* works like this: consider the finite field $F = \mathrm{GF}(p^m)$, let G denote the multiplicative group of F and let α be any primitive element of F. The subset D of G defined by

$$D = \{\alpha^{2i+1} - 1\}_{i=0}^{k-1} \tag{40}$$

where

$$k = \tfrac{1}{2}(p^m - 1) \tag{41}$$

is an almost difference set (see [22] for a proof). The binary sequence that corresponds to D according to equation (10) is an almost perfect sequence with correlations

$$C_g = \begin{cases} 2 \text{ or } -2 & \text{if } k \text{ is odd} \\ 0 \text{ or } -4 & \text{if } k \text{ is even.} \end{cases} \tag{42}$$

For example $p = 7$ and $m = 1$: GF(7) is equivalent to $\mathbb{Z}_7$, the integers $0, \ldots, 6$ with addition and multiplication modulo 7. The primitive element $\alpha = 3$ leads to

$$D = \{2, 5, 4\} \tag{43}$$

and the corresponding binary sequence reads

$$S = (-1, -1, +1, -1, +1, +1) \tag{44}$$

with correlations $C_1 = C_2 = C_4 = C_5 = -2$ and $C_3 = +2$.

For $N \equiv 2 \bmod 4$, any almost perfect sequence is a ground state of the Bernasconi model, i.e. the construction of Lempel *et al* yields ground states for $N = 4t + 2 = p^m - 1$, where p is an odd prime. Since our numerical results suggest that almost perfect sequences do exist for all values of N, we arrive at the conjecture, that the ground states of the Bernasconi model for $N = 4t + 2$ are given by almost perfect sequences with ground-state energy $E = 4(N - 1)$. This conjecture is in agreement with former numerical results [6].

For the three other residue classes, the question of whether an almost perfect sequence is a ground state depends on $|U|$, i.e. on the number of correlations that deviate from the optimum value.

Consider first the case $N = 4t + 1$ where t is a positive integer. Let the value $(-1)^i(2i + 1)$ appear $2n_i$ times among the correlations of a sequence, $i = 0, 1, \ldots$. The factor of 2 reflects the fact that $C_g = C_{N-g}$ must hold. The possible excitations above the theoretical minimum energy $E = 4t$ are given by

$$\begin{aligned} \Delta E = \tfrac{1}{16}(E - 4t) &= \tfrac{1}{2} \sum_{i=1}^{\infty} \mathrm{i}(i + 1)n_i \\ &= n_1 + 3n_2 + 6n_3 + 10n_4 + 15n_5 + \cdots . \end{aligned} \tag{45}$$

Since $\sum_{i=0}^{\infty} n_i = 2t$ must hold, the above sum is finite, of course. Equation (5) imposes the constraint

$$\sum_{j=1}^{\infty} j\,(n_{2j} - n_{2j-1}) = \tfrac{1}{2}u(u + 1) - t \tag{46}$$

on the n_i, where u is a non-negative integer. An almost perfect sequence has $n_i = 0$ for $i > 1$ and equation (46) reduces to

$$n_1 = t - \tfrac{1}{2}u(u + 1). \tag{47}$$

This limits the possible values for n_1 to

$$n_1 \in \{t, t - 1, t - 3, \ldots, t - \tfrac{1}{2}u_{\max}(u_{\max} + 1)\} \tag{48}$$

with

$$u_{\max}(t) = \left\lfloor \tfrac{1}{2}\sqrt{1 + 8t} \right\rfloor . \tag{49}$$

We ran a numerical search for low-energy, almost perfect sequences up to size $N = 81$, table 2 shows the result. For $N \leqslant 41$ we perform an exhaustive enumeration to check that the sequences we found are true ground states. Using equation (46), we can assert that any hypothetical sequence with energy below the value listed in table 2 must be an

Table 2. Number of correlations $C_g = -3$ in low-energy, almost perfect, sequences for $N = 4t+1$ found by numerical search. An entry a.p. in column 4 indicates that any hypothetical sequence with lower energy must be an almost perfect sequence. The energy of the sequences is given by $E = 16n_1 + N - 1$.

N	n_1: possible values	Found	Ground state
5	0, 1	0	yes
9	1, 2	1	yes
13	0, 2, 3	0	yes
17	1, 3, 4	3	yes
21	2, 4, 5	2	yes
25	0, 3, 5, 6	3	yes
29	1, 4, 6, 7	4	yes
33	2, 5, 7, 8	2	yes
37	3, 6, 8, 9	3	yes
41	0, 4, 7, 9, 10	4	yes
45	1, 5, 8, 10, 11	5	a.p.
49	2, 6, 9, 11, 12	6	a.p.
53	3, 7, 10, 12, 13	7	?
57	4, 8, 11, 13, 14	8	?
61	0, 5, 9, 12, 14, 15	9	?
65	1, 6, 10, 13, 15, 16	10	?
69	2, 7, 11, 14, 16, 17	11	?
73	3, 8, 12, 15, 17, 18	12	?
77	4, 9, 13, 16, 18, 19	18	?
81	5, 10, 14, 17, 19, 20	19	?

almost perfect sequence for $N = 45$ and $N = 49$. This is not possible for larger values like $N = 53$, where a configuration with $n_1 = 0$ and $n_2 = 1$ has lower energy ($\Delta E = 3$) and satisfies equation (46). For $N = 5$ and $N = 13$, perfect sequences based on Singer difference sets are ground states. Note that the Legendre sequences for $N \equiv 1 \bmod 4$ prime have $n_1 = \frac{1}{4}(N-1)$. This value is too large for a ground state, at least for those values of N considered in table 2.

Based on their numerical results for $N \leqslant 50$, Marinari *et al* [6] observed that

$$\Delta E = t - 6 \tag{50}$$

holds for $t = 8, 9, \ldots, 12$. As can be seen from table 2, this equation seems to hold at least up to $t = 18$ ($N = 73$).

Consider now the case $N = 4t + 3$. This time, $2n_i$ denotes the number of correlations with value $(-1)^{i+1}(2i+1)$. The excitation energy reads

$$\begin{aligned}\Delta E = \tfrac{1}{16}(E - 4t - 2) &= \tfrac{1}{2}\sum_{i=1}^{\infty} \mathrm{i}(i+1)n_i \\ &= n_1 + 3n_2 + 6n_3 + 10n_4 + 15n_5 + \cdots\end{aligned} \tag{51}$$

and equation (5) leads to the constraint

$$\sum_{j=1}^{\infty} j\,(n_{2j} - n_{2j-1}) = \tfrac{1}{2}u(u+1) \tag{52}$$

where u is a non-negative integer. An almost perfect sequence must have

$$n_1 \in \{0, 1, 3, 6, \ldots, \tfrac{1}{2}u_{\max}(u_{\max}+1)\} \tag{53}$$

Table 3. Number of correlations $C_g = 3$ in low-energy, almost perfect, sequences for $N = 4t+3$ found by numerical search. For all other values of $N = 4t + 3 < 75$, ground states are given by perfect sequences based on Hadamard difference sets.

N	n_1: possible values	Found	Ground state
27	1, 3, 6, 10	3	yes
39	1, 3, 6, 10, 15	3	yes
51	1, 3, 6, 10, 15, 21	6	?
55	1, 3, 6, 10, 15, 21	10	?

with

$$u_{\max}(t) = \left\lfloor \tfrac{1}{2}\left(\sqrt{9+16t}-1\right)\right\rfloor. \tag{54}$$

Most values $N = 4t+3 < 75$ allow the construction of Hadamard cyclic difference sets, i.e. perfect sequences. Table 3 lists low-energy sequences found by numerical search for the four remaining values $N < 75$. The numerical search for $N = 75$ yielded low-energy configurations $\Delta E = 14$ with $(n_1, n_2) = (8, 2)$ and $(n_1, n_2) = (11, 1)$. This does of course not exclude the possibility of an almost perfect sequence with lower energy.

4.2. The case $N \equiv 0$ mod 4

So far all known ground states for N odd or $N \equiv 2 \bmod 4$ are perfect or almost perfect sequences. The first exceptions occur for $N = 4t$. Let m_i (n_i) denote the number of correlations with value $4i$ ($-4i$). The excitation above the theoretical minimum $E = 0$ reads

$$\Delta E = \tfrac{1}{16}E = \sum_{i=1} i^2(m_i + n_i) \tag{55}$$

and equation (5) leads to the constraint

$$\sum_{i=1}^{\infty} \mathrm{i}(m_i - n_i) = u^2 - t \tag{56}$$

where u is a non-negative integer.

Table 4 shows low-energy configurations in terms of m_i and n_i, found either by exhaustive enumeration ($N \leqslant 40$) or numerical search. For $N = 28, 32, 36$ and 40, the ground states are not given by almost perfect sequences, but by sequences which still obey $|C_g| \leqslant 4$. For $N = 48, 56, 64$, even these bounds seem to be violated.

The construction of Lempel *et al* [22] for $N = p^m - 1$, p odd prime, yields almost perfect sequences with $n_1 = N/4$. These sequences are not ground states for all values of N in table 4. They do not even have the lowest energy among all almost perfect sequences.

Wolfmann [23] and Potts and Bradley [24] described a construction for $N \equiv 0 \bmod 4$, that yields sequences with all $C_g = 0$, except $C_{N/2} = -(N-4)$. The energy of such sequences is much higher than the ground-state energy, at least for those N considered in table 4.

4.3. Two-prime sequences

In this section, we describe the construction of low-autocorrelation binary sequences for $N = pq$, p and q prime, which can be shown to be true ground states of the Bernasconi

Table 4. Low-energy configurations for $N = 4t$, found by exhaustive enumeration ($N \leqslant 40$) or numerical search.

N	ΔE	m_2	m_1	n_1	n_2	Ground state
8	1	0	0	1	0	yes
12	1	0	1	0	0	yes
16	3	0	0	3	0	yes
20	4	0	0	4	0	yes
		0	4	0	0	yes
24	2	0	0	2	0	yes
28	5	0	1	4	0	yes
32	5	0	3	2	0	yes
36	4	0	2	2	0	yes
40	5	0	2	3	0	yes
44	9	0	7	2	0	?
48	6	1	2	0	0	?
52	8	0	2	6	0	?
56	12	1	4	4	0	?
60	7	0	4	3	0	?
64	14	0	6	4	1	?
68	16	0	12	4	0	?
72	13	0	10	3	0	?
76	17	0	7	10	0	?

model if p and q are twin primes. For general primes p and q, they have at least a low energy, far below the energies that can be found by numerical search for large N.

Let p and q be odd primes and $p > q$. Then $G = \mathbb{Z}_q \times \mathbb{Z}_p$ is a pq-element cyclic (additive) group. Consider the subset $D \subset G$ given by

$$D = \underbrace{\{(a, b) \in G | a, b \neq 0, \chi_q(a) = \chi_p(b)\}}_{=:M} \cup \{(a, 0) \in G | a \in \mathbb{Z}_q\}. \tag{57}$$

D has

$$k = \tfrac{1}{2}(p-1)(q-1) + q \tag{58}$$

elements and M is a multiplicative group.

To calculate the correlations of the two-prime sequence

$$s_i = \begin{cases} +1 & (i \bmod q, i \bmod p) \in D \\ -1 & \text{otherwise,} \end{cases} \tag{59}$$

we generalize the proof given in [25] to arbitrary primes p and q. Note that the sequences given by equations (31) and (59) are the same.

Let $\lambda(x, y)$ denote the number of different representations

$$(x, y) = (a_1, b_1) - (a_2, b_2) \qquad (a_i, b_i) \in D \tag{60}$$

of $(x, y) \in G - \{0\}$. Since $MD = D$, differences (x, y) and $(m_1 x, m_2 y)$ with $(m_1, m_2) \in M$ will occur equally often in D. Hence there are constants λ_1, λ_2, λ_3 and λ_4 such that

$$\lambda(x, y) = \begin{cases} \lambda_1 & \text{for } x, y \neq 0 \text{ and } \chi_q(x) = \chi_p(y) \\ \lambda_2 & \text{for } x, y \neq 0 \text{ and } \chi_q(x) \neq \chi_p(y) \\ \lambda_3 & \text{for } x = 0 \\ \lambda_4 & \text{for } y = 0. \end{cases} \tag{61}$$

The corresponding autocorrelations read

$$C(x, y) = 4\lambda(x, y) - pq + 2(p - q) - 2. \tag{62}$$

To calculate $\lambda_1, \ldots \lambda_4$, we will look closely at the number of difference representations in $\mathbb{Z}_t^*$, the group of integers $1, \ldots, t-1$ with multiplication mod t, t prime. Let $\varepsilon_1, \varepsilon_2 \in \{1, -1\}$ and $x \in \mathbb{Z}_t^*$ and

$$\lambda^t_{\varepsilon_1,\varepsilon_2}(x) = |\{(a_1, a_2)|x = a_1 - a_2, a_1, a_2 \in \mathbb{Z}_t^*, \chi_t(a_i) = \varepsilon_i\}|. \tag{63}$$

Then we have

$$\lambda^t_{\varepsilon_1,\varepsilon_2}(x) = \begin{cases} \lambda^t_{\varepsilon_1,\varepsilon_2}(1) & \text{if } \chi_t(x) = 1 \\ \lambda^t_{-\varepsilon_1,-\varepsilon_2}(1) & \text{if } \chi_t(x) = -1. \end{cases} \tag{64}$$

We define $\lambda^t_{\varepsilon_1,\varepsilon_2} = \lambda^t_{\varepsilon_1,\varepsilon_2}(1)$. We also write $+, -$ instead of $1, -1$. Then clearly

$$\lambda^t_{++} + \lambda^t_{+-} + 1 = \lambda^t_{--} + \lambda^t_{-+} = \frac{t-1}{2}. \tag{65}$$

From equation (25) we deduce

$$\lambda^t_{++} + \lambda^t_{--} - \lambda^t_{+-} - \lambda^t_{-+} = -1. \tag{66}$$

Furthermore, for $\varepsilon \in \{1, -1\}$ we set

$$\delta^t_\varepsilon = \begin{cases} 1 & \text{if } \chi_t(-1) = \varepsilon \\ 0 & \text{else.} \end{cases} \tag{67}$$

We decompose $\mathbb{Z}_t^*$ in intervals of squares resp. non-squares only, i.e.

$$\mathbb{Z}_t^* = \bigcup_{i=1}^{r} [m_{i-1} + 1, \ldots, m_i] \qquad m_0 = 0,\ m_r = t - 1 \tag{68}$$

where $[m_{i-1}+1, \ldots, m_i]$ consists of squares for odd i and of non-squares for even i. Then λ^t_{-+} resp. λ^t_{+-} counts the difference representations $1 = (m_i + 1) - m_i$ for i odd resp. i even, and thus

$$\lambda^t_{-+} - \lambda^t_{+-} = \delta^t_-. \tag{69}$$

The above equations for the parameters $\lambda^t_{\varepsilon_1,\varepsilon_2}$ provide an easily solvable system of linear equations with solution

$$\begin{aligned} \lambda^t_{++} &= \frac{t-1}{4} + \frac{\delta^t_-}{2} - 1 = \left[\frac{t-3}{4}\right] \\ \lambda^t_{--} = \lambda^t_{+-} &= \frac{t-1}{4} - \frac{\delta^t_-}{2} = \left\lceil \frac{t-3}{4} \right\rceil \\ \lambda^t_{-+} &= \frac{t-1}{4} + \frac{\delta^t_-}{2} = \left[\frac{t+1}{4}\right]. \end{aligned} \tag{70}$$

Finally, we define

$$\begin{aligned} \delta^{p,q} &= \begin{cases} 1 & \text{if } \chi_p(-1) = \chi_q(-1) \\ 0 & \text{else} \end{cases} \\ &= \begin{cases} 1 & \text{if } p \equiv q \bmod 4 \\ 0 & \text{else.} \end{cases} \end{aligned} \tag{71}$$

For the value λ_1 we have:

$$\lambda_1 = \lambda(1,1) = \lambda^q_{+-}(\lambda^p_{+-} + 1 + \delta^p_-) + \lambda^q_{-+}(\lambda^p_{-+} + \delta^p_+) + \lambda^q_{++}(\lambda^p_{++} + 1 + \delta^p_+) + \lambda^q_{--}(\lambda^p_{--} + \delta^p_-) + 1 + \delta^{p,q} \tag{72}$$

where in the final term $1 + \delta^{p,q}$ the contribution 1 counts the difference representation $(1,1) = (1,1) - (0,0)$ and $\delta^{p,q}$ counts $(1,1) = (0,0) - (-1,-1)$. Substituting the parameter values obtained above, we then obtain

$$\lambda_1 = \frac{1}{4}(pq - 2(p-q) + 1) + \frac{\delta^{p,q}}{2}. \tag{73}$$

Let $z \in \mathbb{Z}_p^*$ with $\chi_p(z) = -1$. We then obtain the value λ_2 as:

$$\lambda_2 = \lambda(1,z) = \lambda^q_{-+}(\lambda^p_{+-} + 1 + \delta^p_-) + \lambda^q_{+-}(\lambda^p_{-+} + \delta^p_+) + \lambda^q_{--}(\lambda^p_{++} + 1 + \delta^p_+) + \lambda^q_{++}(\lambda^p_{--} + \delta^p_-) + 1 - \delta^{p,q} \tag{74}$$

where the final term $1 - \delta^{p,q}$ counts the difference representation $(1,z) = (0,0) - (-1,-z)$. Substituting our parameter values gives

$$\lambda_2 = \frac{1}{4}(pq - 2(p-q) + 1) - \frac{\delta^{p,q}}{2}. \tag{75}$$

Furthermore,

$$\begin{aligned} \lambda_3 &= \lambda(0,1) \\ &= (\lambda^p_{++} + \lambda^p_{--})\frac{q-1}{2} + q - 1 \\ &= \tfrac{1}{4}(p+1)(q-1) \end{aligned} \tag{76}$$

and

$$\begin{aligned} \lambda_4 &= \lambda(1,0) \\ &= (\lambda^q_{++} + \lambda^q_{--})\frac{p+1}{2} + \lambda^q_{+-} + \lambda^q_{-+} + 2 \\ &= \tfrac{1}{4}(q-3)(p-1) + q. \end{aligned} \tag{77}$$

The correlations for $g \neq 0$ finally read

$$C_g = \begin{cases} -1 + 2\delta^{p,q} & \text{for } \chi_q(g) = \chi_p(g),\ g \not\equiv 0 \bmod p, q \\ -1 - 2\delta^{p,q} & \text{for } \chi_q(g) \neq \chi_p(g),\ g \not\equiv 0 \bmod p, q \\ p - q - 3 & \text{for } g \equiv 0 \bmod q \\ q - p + 1 & \text{for } g \equiv 0 \bmod p \end{cases} \tag{78}$$

with

$$E = (1 + 4\delta^{p,q})(p-1)(q-1) + (p-q-3)^2(p-1) + (p-q-1)^2(q-1). \tag{79}$$

For $p - q = 2$, all correlations are -1, i.e. we proved that the twin-prime sequence equation (31) corresponds to a cyclic Hadamard difference set. For $p - q > 2$, the construction does not necessarily lead to a ground state, as can be seen for $N = 21, 33, 57, 65, 69$ (table 2) and $N = 39, 51, 55$ (table 3). Nevertheless two-prime sequences have energies well below those found by extensive numerical search for large $N = pq$ and small difference $p - q$.

4.4. Jacobi sequences

The *Jacobi symbol* $\psi_N(j)$ is a generalization of the quadratic character $\chi_p(j)$ (equation (23)) to the case in which $N = p_1^{r_1} p_2^{r_2} \dots p_s^{r_s}$ is the product of odd primes:

$$\psi_N(j) = \prod_{i=1}^{s} \chi_{p_i}^{r_i}(j). \tag{80}$$

Note that $\psi_N(j) = 0$ if $(j, p_i) = 0$, i.e. if j is divided by p_i. The number of such zeros in the range $0 \dots N-1$ is given by $N - \phi(N)$, where Euler's totient function $\phi(N)$ is defined as the number of positive integers smaller than N that are coprime to N. In our case we have

$$\phi(N) = \prod_{i=1}^{s} p_i^{r_i - 1}(p_i - 1). \tag{81}$$

A *Jacobi sequence* is a ± 1 sequence of length N, given by

$$s_j = \begin{cases} \psi_N(j) & \text{if } \psi_N(j) \neq 0 \\ \pm 1 & \text{if } \psi_N(j) = 0. \end{cases} \tag{82}$$

Setting the zeros of the Jacobi symbol to ± 1 leads to $2^{N-\phi(N)}$ distinct sequences.

Jacobi sequences are potential candidates for low-energy configurations, for three reasons. First, the Jacobi sequences reduce to the Legendre sequences for N prime. Second, for $N = p_1 p_2$ and a special choice for the zeros of the Jacobi symbol, we rediscover the two-prime sequences, equation (31). Third, Borsari *et al* [26] have shown that the Jacobi sequences are ground states of the sine model, equation (30), for $N = 4t + 3$ and not divisible by a square.

To check the suitability of the Jacobi sequences as low-energy configurations for the Bernasconi model, we did an exhaustive enumeration of all $2^{N-\phi(N)}$ Jacobi sequences of fixed length $N = pq$ to find the sequence with minimum energy. Table 5 displays the result. The two-prime sequences are special Jacobi sequences, so their energy can not be lower than the Jacobi energy. The data from table 5 indicates that the two-prime sequences have minimum energy among all Jacobi sequences for $p - q \leqslant 6$. For larger values of $p - q$, the energy of the two-prime sequences is larger. On the other hand, the discrepancy between the Jacobi energy and the ground-state energy is clearly visible. Except for the twin-prime case, Jacobi sequences are not ground states of the Bernasconi model. This discrepancy is even larger for non-square-free values of N (table 6).

This is no surprise, since prime powers dividing N lead to regularities in the Jacobi symbol which keep the correlation values high. As an example consider $N = p^r$. In this case ψ is periodic, $\psi_N(j + p) = \psi_N(j)$, and we obtain

$$C_k \geqslant p^{r-1}(p-2) \qquad \text{if } k \equiv 0 \bmod p \tag{83}$$

for all Jacobi sequences.

5. Summary and open problems

We have demonstrated that the ground states of the Bernasconi model with periodic boundary conditions are closely related to cyclic or almost cyclic difference sets. Using theorems and well-founded conjectures from the theory of cyclic difference sets together with exact enumerations and numerical searches, we obtain some results on the ground states of the Bernasconi model, which are conveniently summarized by the following facts and conjectures.

Table 5. Energies of configurations for $N = p*q$, p, q odd primes and $p > q+2$. For $p = q+2$, twin-prime sequences are ground states. The column 'Jacobi' contains the minimum enery of all Jacobi sequences for given N, obtained by exhaustive enumeration of all $2^{N-\phi(N)} = 2^{p+q-1}$ such sequences.

			Energies		
N	p	q	Two-prime	Jacobi	Ground state
21	7	3	84	84	42
33	11	3	228	208	64
39	13	3	774	342	86
51	17	3	2 306	610	$\leqslant$146
55	11	5	230	230	$\leqslant$214
57	19	3	3 672	648	$\leqslant$184
65	13	5	736	592	$\leqslant$224
69	23	3	7 300	964	$\leqslant$244
77	11	7	364	364	$\leqslant$364
85	17	5	2 100	1076	$\leqslant$324
87	29	3	16 118	1718	$\leqslant$438
91	13	7	330	330	$\leqslant$330
93	31	3	20 508	1788	$\leqslant$764
95	19	5	2 926	1102	$\leqslant$894

Table 6. Minimum energies of Jacobi sequences for odd, non-squarefree values of $N < 100$, compared with the ground-state energies of the Bernasconi model.

N	Jacobi	Ground state
9	56	24
25	3 000	72
27	3 802	74
45	1 372	$\leqslant$124
49	2 055	$\leqslant$144
63	2 622	62
75	17 354	$\leqslant$298

Fact 1. Perfect binary sequences, equation (13), do exist and form ground states of the Bernasconi model for $N = 4, 5, 6, 13$, $N = 2^j - 1$ with $j > 1$, $N = 4t + 3$ prime, $N = p(p + 2)$ with both p and $p + 2$ prime.

This fact can be proven using the known constructions for cyclic difference sets, as has been shown in section 3.

Conjecture 1. For all values of N that do not match any of the conditions in fact 1, there is no perfect sequence, i.e. ground states are formed by non-perfect sequences.

This conjecture has a very solid base in the various non-existence theorems for cyclic difference sets as cited in section 3.

Conjecture 2. Almost perfect sequences exist for all values of N.

Beside those values of N that match a condition in fact 1, this can be proven for $N = 4t+1$ prime (Legendre sequence) and $N = q - 1$, where q is an odd prime power (construction of Lempel *et al*). For other values of N, we checked this conjecture numerically up to $N < 84$.

Conjecture 3. For $N \equiv 2 \bmod 4$, the ground states of the Bernasconi model are given by almost perfect sequences. The ground-state energy is $E = 4(N-1)$. For other values of N, the ground-state energy obeys

$$E \leqslant \begin{cases} 16(N-1) & \text{for } N \equiv 0 \bmod 4 \\ 9(N-1) & \text{for } N \equiv 3 \bmod 4. \end{cases} \tag{84}$$

This follows immediately from conjecture 2.

Conjecture 4. For $N \equiv 1 \bmod 4$, almost perfect sequences are ground states of the Bernasconi model. The ground-state energy is $E = 5(N-1) - 8u(u+1)$, where u is a non-negative integer $\leqslant \frac{1}{2}\sqrt{2N-1}$.

This conjecture is based on the numerical results from table 2. For the thermodynamic limit, our results lead us to the following conjecture.

Conjecture 5. The ground-state energy of the Bernasconi model is $\mathrm{O}(N)$. The limit $\lim_{N\to\infty} \frac{E(N)}{N}$ is however not well defined, since the precise value of $E(N)$ depends on number theoretic properties of N.

This result is very different from the situation for the Bernasconi model with aperiodic boundary conditions, where $E(N) = \mathrm{O}(N^2)$, and $\lim_{N\to\infty} \frac{E(N)}{N^2}$ seems to be well defined [7].

Marinari *et al* [6] noticed some patterns in their numerical results for the ground-state energies for $N \leqslant 50$. Their equation (12) is a special case of conjecture 2. Equation (13) of [6] is equivalent to conjecture 4 with fixed value $u = 3$ for $N \geqslant 33$. Our numerical results (table 2) support this special value of u up to $N = 73$. For $N = 77$ and $N = 88$ we only found $u \leqslant 1$.

We did not find sequences with lower energies than those reported in [6]. This is due to the fact that numerical methods such as the one applied by Marinari *et al* work quite well if N is not too large ($N \leqslant 50$). Our experience with numerical search suggests that beyond $N > 100$ true ground states can only be found by mathematical insight rather than computer power.

One step towards more mathematical insight is to prove or disprove the above conjectures. Especially the conjecture on the existence of almost perfect sequences for all values of N deserves some attention. Another open problem is the generalization of successful construction methods for special N to more general values. Here, the method of Lempel *et al* [22] is the most interesting candidate.

Acknowledgment

The authors appreciate fruitful discussions with Alexander Pott.

References

[1] Schroeder M R 1984 *Number Theory in Science and Communication (Springer Series in Information Sciences)* (Berlin: Springer)
[2] Golay M J E 1982 The merit factor of long low autocorrelation binary sequences *IEEE Trans. Inf. Theory* **28** 543
[3] Bernasconi J 1987 Low autocorrelation binary sequences: statistical mechanics and configuration space analysis *J. Physique* **48** 559
[4] Krauth W and Mézard M 1995 Aging without disorder on long time scales *Z. Phys.* B **97** 127–31

[5] Bouchaud J P and Mézard M 1994 Self induced quenched disorder: a model for the glass transition *J. Physique* I **4** 1109–14
[6] Marinari E, Parisi G and Ritort F 1994 Replica field theory for determistic models: I. Binary sequences with low autocorrelation. *J. Phys. A: Math. Gen.* **27** 7615–45
[7] Mertens S 1996 Exhaustive search for low-autocorrelation binary sequences *J. Phys. A: Math. Gen.* **29** L473–81
[8] Ground states for open boundary conditions up to $N = 50$ can be downloaded from http://itp.nat.uni-magdeburg.de/~mertens/bernasconi/open.dat
[9] Baumert L D 1971 *Cyclic Difference Sets* (Berlin: Springer)
[10] Jungnickel D 1992 Difference sets *Contemporary Design Theory: A Collection of Surveys* ed J H Dinitz and D R Stinson (New York: John Wiley) pp 241–324
[11] Pott A 1995 *Finite Geometry and Character Theory (Lecture Notes in Mathematics 1601)* (Berlin: Springer)
[12] Song H Y and Golomb S W 1994 On the existence of cyclic Hadamard difference sets *IEEE Trans. Inf. Theory* **40** 1266–8
[13] Jungnickel D 1993 *Finite Fields: Structure and Arithmetics* (Mannheim: Bibliographisches Institut)
[14] Watson E J 1962 Primitive polynomials (mod 2) *Math. Comput.* **16** 368–9
[15] Živković M 1994 A table of primitive binary polynomials *Math. Comput.* **62** 385–6
[16] Živković M 1994 Table of primitive binary polynomials. II. *Math. Comput.* **63** 301–6
[17] Marinari E, Parisi G and Ritort F 1994 Replica field theory for determistic models: II. A non-random spin glass with glassy behaviour *J. Phys. A: Math. Gen.* **27** 7647–68
[18] Schmidt B 1997 Circulant Hadamard matrices: Overcoming non-self-conjugacy *Preprint* Mathematisches Institut, Universität Augsburg
[19] Turyn R and Storer J 1961 On binary sequences *Proc. Am. Math. Soc.* **12** 394–9
[20] Turyn R 1968 Sequences with small correlation *Error Correcting Codes* ed H B Mann (New York: Wiley) pp 195–228
[21] Eliahou S and Kervaire M 1992 Barker sequences and difference sets *L'Ens. Math.* **38** 345–82
[22] Lempel A, Cohn M and Eastman W 1977 A class of balanced binary sequences with optimal autocorrelation properties *IEEE Trans. Inf. Theory* **23** 38–42
[23] Wolfmann J 1992 Almost perfect autocorrelation sequences *IEEE Trans. Inf. Theory* **38** 1412–18
[24] Pott A and Bradley S P 1995 Existence and nonexistence of almost-perfect autocorrelation sequences *IEEE Trans. Inf. Theory* **41** 301–4
[25] Beth T, Jungnickel D and Lenz H 1985 *Design Theory* (Mannheim: Bibliographisches Institut)
[26] Borsari I, Graffi S and Unguendoli F 1996 Ground states for a class of deterministic spin models with glassy behaviour *J. Phys. A: Math. Gen.* **29** 1593–604