ACTA ARITHMETICA
141.2 (2010)

Exact solutions to Waring's problem for finite fields

by

Arne Winterhof (Linz) and Christiaan van de Woestijne (Graz)

1. Introduction and results. Let $q = p^r$ be a power of a prime p and denote by $\mathbb{F}_q$ the finite field of q elements. For a positive integer k, *Waring's problem* for $\mathbb{F}_q$ is the question how many summands are maximally needed to express any given element a of $\mathbb{F}_q$ in the form

$$a = \sum_{i=1}^{g} x_i^k \tag{1.1}$$

with $x_i \in \mathbb{F}_q$, i.e., as a sum of kth powers of elements of $\mathbb{F}_q$. We can then define the *Waring function* $g(k,q)$ as the maximal number of summands needed to express all elements of $\mathbb{F}_q$ as sums of kth powers.

We note that, by an easy argument, we have $g(k,q) = g(k',q)$, where $k' = \gcd(k, q-1)$. Hence, we will assume from now on that k divides $q-1$.

Several authors have established bounds on the value of $g(k,q)$ for various choices of the parameters k and q; a survey is given in [8]. For the cases where the exponent k is small compared to q, there are strong results. For example, whenever $2 \le k < q^{1/4}+1$, it follows that $g(k,q) = 2$ by a direct application of the Weil bound for the number of points on varieties over finite fields [6, 7, 8].

In this paper, we will look at the cases where the exponent k is *large* compared to q, where the known results are weaker. We will obtain not only a bound, but the *exact value* of $g(k,q)$ for two infinite families of pairs (k,q). Our main results are the following.

Theorem 1.2. *Let p and r be primes such that p is a primitive root modulo r. Then*

$$g\left(\frac{p^{r-1}-1}{r}, p^{r-1}\right) = \frac{(p-1)(r-1)}{2}.$$

2010 *Mathematics Subject Classification*: Primary 11P05; Secondary 11T71, 90C10, 94B65.
Key words and phrases: equations over finite fields, Waring's problem, covering radius, Lee metric, exact values.

DOI: 10.4064/aa141-2-3

THEOREM 1.3. *Let p and r be odd primes such that p is a primitive root modulo r. Then*

$$g\left(\frac{p^{r-1}-1}{2r}, p^{r-1}\right) = \begin{cases} \left\lfloor \frac{pr}{4} - \frac{p}{4r} \right\rfloor & \text{if } r < p, \\ \left\lfloor \frac{pr}{4} - \frac{r}{4p} \right\rfloor & \text{if } r \geq p. \end{cases}$$

REMARKS.

1. Theorem 1.2 improves the lower bound of [9, Theorem 2].
2. The value $g(p-1,p) = p-1$ can be regarded as complement of Theorem 1.2 in the case $r = 1$.
3. The values $g((p-1)/2, p) = (p-1)/2$ and $g((p^2-1)/4, p^2) = p-1$ if $p \equiv 3 \pmod 4$ can be regarded as complements of Theorem 1.3 in the case $r = 1$ or $r = 2$, respectively.

The proofs of our results rest on the resolution (Theorems 2.5 and 2.6) of two instances of a combinatorial problem, which will be given in detail in the next section. The problem can be formulated as the determination of the covering radius of cyclic codes in several metrics, including the so-called *Lee metric* (in place of the usual Hamming metric) [1]. There is also a connection with the determination of the diameter of *Waring graphs* in graph theory [4].

Section 3 is devoted to the proof of Theorem 2.5. The proof of Theorem 2.6, which implies Theorem 1.3, is much more involved. In Section 4 we prove that the values given in this theorem are *upper bounds* for the Waring function, while in Section 5 we show that the bounds are attained.

Everything is put together in Section 6. The proof is constructive, in the sense that it gives an algorithm to construct elements in $\mathbb{F}_q$ that need a maximal number of terms to express them as sums of kth powers. An implementation of this algorithm using the KASH computer algebra system (version 2.x) is available from the second author's homepage [10].

2. A combinatorial reformulation. Let m and r be positive integers, and consider the free $\mathbb{Z}/m\mathbb{Z}$-module

$$V = (\mathbb{Z}/m\mathbb{Z})^r.$$

Let $g_1, \ldots, g_r$ be a basis of V, and define V' as the quotient of V by the relation $g_1 + \cdots + g_r = 0$. Then every element v of V' has multiple representations

$$v = \sum_{i=1}^{r} v_i g_i \quad (v_i \in \mathbb{Z}/m\mathbb{Z}), \tag{2.1}$$

and one is interested in the size of the most economical representation. Here, "economical" of course must be defined, and we will do this in two distinct ways.

The first definition that we use assigns to each element x of $\mathbb{Z}/m\mathbb{Z}$ its least residue modulo m, denoted by $\bar{x} \in \{0, 1, \dots, m-1\}$, and looks at

$$\|(v_1, \dots, v_r)\|_1 := \sum_{i=1}^{r} \bar{v}_i.$$

The second uses the absolute least residue modulo m,

$$|x| = \min\{\bar{x}, m - \bar{x}\},$$

and looks at the *Lee norm*

$$\|(v_1, \dots, v_r)\|_2 := \sum_{i=1}^{r} |v_i|.$$

It is clear that if the coefficients $(v_1, \dots, v_r)$ and $(v_1', \dots, v_r')$ both represent the same element v in the form (2.1), then we have

$$(v_1', \dots, v_r') = (v_1, \dots, v_r) + x\mathbf{e}$$

for some $x \in \mathbb{Z}/m\mathbb{Z}$, where $\mathbf{e}$ denotes the vector $(1, \dots, 1)$.

We now give the precise definition of "economic". We call a vector in V *admissible* if

$$\|\mathbf{v}\|_i \le \|\mathbf{v} + x\mathbf{e}\|_i \qquad \text{for all } x \in \mathbb{Z}/m\mathbb{Z},$$

where i is either 1 or 2, depending on the context. The problem to be solved is the following, where "norm" is one of $\|\cdot\|_1$ or $\|\cdot\|_2$.

PROBLEM 2.2. Given positive integers m and r, what is the largest possible norm of an admissible vector in $(\mathbb{Z}/m\mathbb{Z})^r$?

We will provide a complete answer to this question. Define the *norm bound functions* $g(m, r)$ and $h(m, r)$ for positive integers m and r by

$$g(m, r) = \frac{mr - m - r + \gcd(m, r)}{2}; \tag{2.3}$$

$$h(m, r) = \begin{cases} mr/4 & \text{if } m \text{ and } r \text{ are even,} \\ \lfloor mr/4 - 1/2 \rfloor & \text{if } m \text{ is even, } r \text{ is odd, and } r > m, \\ \lfloor mr/4 - r/4m \rfloor & \text{if } m \text{ is odd and } r > m, \\ \lfloor mr/4 - 1/2 \rfloor & \text{if } m \text{ is odd, } r \text{ is even, and } r < m, \\ \lfloor mr/4 - m/4r \rfloor & \text{if } r \text{ is odd and } r \le m. \end{cases} \tag{2.4}$$

Note that $g(m, r)$ is always an integer.

THEOREM 2.5. *Let m and r be positive integers, and let $\mathbf{v}$ be an admissible vector in $V = (\mathbb{Z}/m\mathbb{Z})^r$ of maximal norm $\|\mathbf{v}\|_1$. Then*

$$\|\mathbf{v}\|_1 = g(m, r).$$

THEOREM 2.6. *Let m and r be positive integers, and let $\mathbf{v}$ be an admissible vector in $V = (\mathbb{Z}/m\mathbb{Z})^r$ of maximal Lee norm $\|\mathbf{v}\|_2$. Then*

$$\|\mathbf{v}\|_2 = h(m,r).$$

See the next sections for the proofs of these results.

We note that Problem 2.2 given above can be reinterpreted in terms of covering radii of linear codes, with respect to the Lee metric. This link was also observed by Helleseth in [5].

The covering radius is a fundamental parameter of a code and has extensively been studied. For example the subject is treated in the survey [2] and in the monograph [3]. For the Lee metric in coding theory, we also refer to [1]. Let $C \subseteq (\mathbb{Z}/m\mathbb{Z})^r$ be a code over $\mathbb{Z}/m\mathbb{Z}$ of length r. We say that a vector is *ρ-covered* by a code if it has Lee distance at most ρ from at least one codeword. (The *Lee distance* of $(a_1,\dots,a_r),(b_1,\dots,b_r) \in (\mathbb{Z}/m\mathbb{Z})^r$ is $\sum_{i=1}^r |a_i - b_i|$, where $|x| = \min(\bar{x}, m-\bar{x})$ for $x \in \mathbb{Z}/m\mathbb{Z}$, so it coincides with $\|(a_1-b_1,\dots,a_r-b_r)\|_2$, where $\|\cdot\|_2$ is as defined above.) The *covering radius* is the smallest ρ such that every vector of $(\mathbb{Z}/m\mathbb{Z})^r$ is ρ-covered.

Now let $\mathbf{e}$ be the all-one vector of $(\mathbb{Z}/m\mathbb{Z})^r$. Obviously, for the covering radius ρ of the code $C = (\mathbb{Z}/m\mathbb{Z})\mathbf{e}$ in the Lee metric we have

$$\rho = \begin{cases} g(m,r) = h(m,r) & \text{if } m = 2, \\ h(m,r) & \text{if } m > 2. \end{cases}$$

The Lee distance, and hence the covering radius based on it, is in general different from the Hamming distance; they coincide when $m = 2$ or 3.

We can also interpret $g(m,r)$ and $h(m,r)$ as diameters of the graphs with vertex set V' where two vertices α and β are connected if and only if $\alpha - \beta \in S$ or $\in S \cup -S$, respectively (cf. [4] for prime m). Here S is the set $\{g_1,\dots,g_r\}$ of generators of V'.

3. Proof of Theorem 2.5. We must solve the linear programming problem that asks to maximise $\|\mathbf{v}\|_1$ under

$$\|\mathbf{v}\|_1 \le \|\mathbf{v} + x\mathbf{e}\|_1 \qquad \text{for all } x \in \mathbb{Z}/m\mathbb{Z}.$$

Now since

$$\|\mathbf{v} + x\mathbf{e}\|_1 \equiv \|\mathbf{v}\|_1 + r\bar{x} \pmod{m},$$

the conditions of the problem may be sharpened to

$$\|\mathbf{v}\|_1 \le \|\mathbf{v} + x\mathbf{e}\|_1 - \overline{rx} \qquad \text{for all } x \in \mathbb{Z}/m\mathbb{Z}, \tag{3.1}$$

where $\overline{rx}$, as above, denotes the remainder of rx upon division by m. Since each coordinate of $\mathbf{v} + x\mathbf{e}$ runs through all elements of $\mathbb{Z}/m\mathbb{Z}$ as x runs

through $\mathbb{Z}/m\mathbb{Z}$, summing (3.1) over $x \in \mathbb{Z}/m\mathbb{Z}$ yields

$$m\|\mathbf{v}\|_1 \le r \sum_{x\in\mathbb{Z}/m\mathbb{Z}} \overline{x} - \sum_{x\in\mathbb{Z}/m\mathbb{Z}} \overline{rx} = \binom{m}{2} r - \gcd(m,r)^2 \binom{m/\gcd(m,r)}{2}$$
$$= \frac{m((r-1)(m-1)+\gcd(m,r)-1)}{2}.$$

Obviously, this upper bound is attained by a vector $\mathbf{v}$ with

$$t_k := \frac{\overline{r(k-1)} + r - \overline{rk}}{m}$$

coordinates equal to $m-k$ for $k \in \mathbb{Z}/m\mathbb{Z} \setminus \{0\}$ and all other coordinates equal to zero. Namely, for $x \in \mathbb{Z}/m\mathbb{Z} \setminus \{0\}$ we have

$$\|\mathbf{v} + x\mathbf{e}\|_1 = \|\mathbf{v} + (x-1)\mathbf{e}\|_1 + r - mt_x = \|\mathbf{v}\|_1 + \overline{r(x-1)} + r - mt_x$$
$$= \|\mathbf{v}\|_1 + \overline{rx}$$

by induction and thus equality in (3.1). ∎

4. Upper bounds. In this section and the next we prove Theorem 2.6. Propositions 4.3 and 4.11 will show that the values taken by the function $h(m,r)$ indeed give an upper bound for the norm $\|\cdot\|_2$ of an admissible vector in all cases. Throughout this section, we will write $\|\cdot\|$ for $\|\cdot\|_2$.

We start with some preliminary results.

LEMMA 4.1. *We have*

$$\sum_{x\in\mathbb{Z}/m\mathbb{Z}} |x| = \begin{cases} m^2/4 & \text{if } m \text{ is even,} \\ (m^2-1)/4 & \text{if } m \text{ is odd.} \end{cases}$$

The proof is left to the reader.

LEMMA 4.2. *Let m be even. Then for any $\mathbf{v} \in V$, we have $\|\mathbf{v} + x\mathbf{e}\| \equiv \|\mathbf{v}\| + rx \pmod 2$ for all $x \in \mathbb{Z}/m\mathbb{Z}$.*

Proof. For even m, we have $|c+x| \equiv |c| + x \pmod 2$ for all $c, x \in \mathbb{Z}/m\mathbb{Z}$. ∎

The following proposition gives upper bounds that are the right ones whenever $r \ge m$, and also whenever r is even. For the cases where r is odd and less than m, the bounds given in Proposition 4.11 are better (see also Section 6).

PROPOSITION 4.3. *Let $\mathbf{v} \in V$ be admissible. We have*

$$\|\mathbf{v}\| \le \begin{cases} mr/4 - r/4m & \text{if } m \text{ is odd,} \\ mr/4 & \text{if } m \text{ and } r \text{ are both even,} \\ mr/4 - 1/2 & \text{if } m \text{ is even and } r \text{ is odd.} \end{cases}$$

Proof. We sum the inequalities $\|\mathbf{v} + x\mathbf{e}\| \geq \|\mathbf{v}\|$ over all $x \in \mathbb{Z}/m\mathbb{Z}$. By Lemma 4.1, this yields

$$m\|\mathbf{v}\| \leq \begin{cases} (m^2-1)r/4 & \text{if } m \text{ is odd,} \\ m^2 r/4 & \text{if } m \text{ is even.} \end{cases}$$

This can be sharpened if m is even and r is odd. Namely, by Lemma 4.2, we find the sharper inequality

$$\|\mathbf{v} + x\mathbf{e}\| \geq \|\mathbf{v}\| + (x \bmod 2);$$

by summing over x, we get

$$m\|\mathbf{v}\| \leq m^2 r/4 - m/2.$$

Now division by m yields the result in all cases. ∎

We now embark on the subcase where the dimension r is odd and at most equal to m, as we will need to strengthen the bounds in Proposition 4.3 for this case. Here, much more preparation is needed; the argument is concluded in Proposition 4.11.

Definition 4.4. For a vector $\mathbf{v} \in V$, we define the *norm sequence* of $\mathbf{v}$, written $(N_x(\mathbf{v}))$ or simply (N_x) where x runs over $\mathbb{Z}/m\mathbb{Z}$, by setting $N_x = \|\mathbf{v} + x\mathbf{e}\|$.

Lemma 4.5. *Let r be odd, and let $\mathbf{v} \in V$. If m is even, then $N_{x+1} \neq N_x$ for all $x \in \mathbb{Z}/m\mathbb{Z}$. If m is odd and the number of distinct components of $\mathbf{v}$ is s, then there are at most s values of x in $\mathbb{Z}/m\mathbb{Z}$ for which $N_{x+1} = N_x$.*

Proof. For m even, the result follows easily from Lemma 4.2.

Suppose m is odd. As r is odd, we cannot have $N_{x+1} = N_x$ unless we have $|v_i + x + 1| = |v_i + x|$ for at least one i with $1 \leq i \leq r$. But this implies $v_i + x = (m-1)/2$. Therefore, if $\mathbf{v}$ has s distinct components, there can exist at most s distinct $x \in \mathbb{Z}/m\mathbb{Z}$ with $N_{x+1} = N_x$. ∎

The next two lemmas deal with the horizontal symmetry or near-symmetry of the norm sequence; they are applied in Lemma 4.8. The detailed first assertions of both are again used in Section 5.1. For $x \in \mathbb{Z}/m\mathbb{Z}$, we will write $\bar{x}$ for the representative of x in the set $\{0, 1, \ldots, m-1\} \subseteq \mathbb{Z}$, as before.

Lemma 4.6. *Let m be even. For all $x \in \mathbb{Z}/m\mathbb{Z}$, we have*

$$|x| + \left|x + \frac{m}{2}\right| = \frac{m}{2}.$$

For all $\mathbf{v} \in V$, we have

$$\|\mathbf{v}\| + \left\|\mathbf{v} + \frac{m}{2} \cdot \mathbf{e}\right\| = \frac{mr}{2}.$$

Proof. If $0 \le \bar{x} < m/2$, then $|x|+|x+m/2| = \bar{x}+m-(\bar{x}+m/2) = m/2$. If $m/2 \le \bar{x} < m$, then $|x| + |x + m/2| = m - \bar{x} + (\bar{x} + m/2 - m) = m/2$. The last assertion follows by the definition of the Lee norm. ∎

LEMMA 4.7. *Let m be odd. For all $x \in \mathbb{Z}/m\mathbb{Z}$, we have*

$$\text{(i)}\quad |x| + \left|x + \frac{m+1}{2}\right| = \begin{cases} (m-1)/2 & \text{if } 0 \le \bar{x} \le (m-1)/2, \\ (m+1)/2 & \text{if } (m+1)/2 \le \bar{x} \le m-1; \end{cases}$$

$$\text{(ii)}\quad |x| + \left|x + \frac{m-1}{2}\right| = \begin{cases} (m-1)/2 & \text{if } x=0 \text{ or } (m+1)/2 \le \bar{x} \le m-1, \\ (m+1)/2 & \text{if } 1 \le \bar{x} \le (m-1)/2. \end{cases}$$

For all $\mathbf{v} \in V$, we have

$$2\|\mathbf{v}\| + \left\|\mathbf{v} + \frac{m-1}{2}\cdot\mathbf{e}\right\| + \left\|\mathbf{v} + \frac{m+1}{2}\cdot\mathbf{e}\right\| = mr - \#\{i \mid v_i = 0\}.$$

Proof. If $0 \le \bar{x} \le (m-1)/2$, then $|x| = \bar{x}$ and $|\bar{x} + (m+1)/2| = m - (\bar{x} + (m+1)/2)$, while if $(m+1)/2 \le \bar{x} \le m-1$, then $|x| = m - \bar{x}$ and $|x + (m+1)/2| = (\bar{x} + (m+1)/2) - m$.

We have $|0| + |(m-1)/2| = (m-1)/2$. Also, if $1 \le \bar{x} \le (m-1)/2$, then $|x| = \bar{x}$ and $|x + (m-1)/2| = m - (\bar{x} + (m-1)/2)$. Finally, if $(m+1)/2 \le \bar{x} \le m-1$, then $|x| = m - \bar{x}$ and $|x + (m-1)/2| = (\bar{x} + (m-1)/2) - m$.

As to the last assertion, let $\mathbf{v} = (v_1, \dots, v_r) \in V$ and let $1 \le i \le r$. By the first part, we have

$$(|v_i| + |v_i + (m-1)/2|) + (|v_i| + |v_i + (m+1)/2|) = m,$$

unless the two summands are equal. Now these two summands being both equal to $(m-1)/2$ implies $v_i = 0$, and they cannot be both $(m+1)/2$. The claim follows by the definition of the Lee norm. ∎

LEMMA 4.8. *Let $\mathbf{v} \in V$ be admissible. Then for all $x \in \mathbb{Z}/m\mathbb{Z}$, we have*

$$\|\mathbf{v} + x\mathbf{e}\| \le mr/2 - \|\mathbf{v}\|.$$

Proof. First, suppose that m is even, and apply Lemma 4.6 to $\mathbf{v} + x\mathbf{e}$. By admissibility, we have $\|\mathbf{v} + (x + m/2)\mathbf{e}\| \ge \|\mathbf{v}\|$, and the result follows.

If m is odd, we apply Lemma 4.7 to $\mathbf{v} + x\mathbf{e}$ and use the admissibility inequality for both $\mathbf{v} + (x + (m-1)/2)\mathbf{e}$ and $\mathbf{v} + (x + (m+1)/2)\mathbf{e}$. After dividing by 2, we obtain the result. ∎

DEFINITION 4.9. Let $(a_x)_{x \in \mathbb{Z}/m\mathbb{Z}}$ be a sequence of real numbers. We define the *slope* of (a_x) at x to be $a_{x+1} - a_x$. We say that the sequence has a *maximum* at x if there exists $c \in \{1, 2, \dots, m-1\}$ such that

$$a_{x-1} < a_x, \quad a_{x+i} = a_x \quad \text{for } i = 0, 1, \dots, c-1, \quad a_{x+c} < a_x.$$

A *minimum* is defined symmetrically; and we define an *extremal value* to be either a minimum or a maximum.

LEMMA 4.10. *Let $\mathbf{v} \in V$, and let (N_x) be the norm sequence of $\mathbf{v}$. If the number of distinct components of $\mathbf{v}$ is s, then the number of extremal values of the sequence (N_x) is at most $2s$.*

Note that this result is independent of the parities of m and r. For the multiplication by 2 used in the proof of the second part, see also Section 5.3.

Proof. Recall that all sequences in this proof are periodic with period m. The sequence (N_x) is the sum of the sequences $(|v_i + x|)$, where i runs over $1, \ldots, r$.

First, let us consider the case where m is even. Here each period of the composing sequences is made up of two segments; in the first, starting at $x = \overline{-v_i}$, the sequence increases with slope 1, while in the second it decreases with slope -1. We see that the composing sequences only change slope at the two extremal values they possess, which all have $c = 1$ in the notation of Definition 4.9. Now suppose (N_x) has an extremal value at x; then in particular its slope at $x - 1$ and its slope at x are different, so one of the composing sequences must change its slope as well. It follows that also one of the composing sequences has an extremal value at x, and consequently x must be equal to one of the at most $2s$ values where such an extremal value occurs.

Second, assume m is odd; we will reduce this case to the previous one, as follows. Let (S_x) be any sequence of real numbers indexed by the integers modulo m, and suppose (T_y) is any real sequence, indexed by the integers modulo $2m$, such that $T_y = S_{y/2}$ whenever y represents an even class modulo $2m$. We claim that the sequence (T_y) has no fewer extremal values than the sequence (S_x). Indeed, suppose (S_x) has a maximum at x, and consider the subsequence $T_{2x-2} = S_{x-1}, T_{2x-1}, T_{2x} = S_x, \ldots, T_{2x+2c-1}, T_{2x+2c}$ of (T_y). Let y be the first index with T_y as large as possible in this subsequence. Then as $T_{y-1} < T_y$ and $T_{2x+2c} < T_y$, the sequence (T_y) has a maximum at y, possibly with a smaller value of c. This proves the claim.

We apply the claim to the norm sequence (N_x) of $\mathbf{v}$ and the sequence $(M_y)_{y \in \mathbb{Z}/2m\mathbb{Z}}$ with $M_y = \frac{1}{2}\|2\mathbf{v} + y\mathbf{e}\|$ for $y \in \mathbb{Z}/2m\mathbb{Z}$; here $2\mathbf{v}$ means the image of $\mathbf{v}$ under the $\mathbb{Z}$-linear map $(\mathbb{Z}/m\mathbb{Z})^r \to (\mathbb{Z}/2m\mathbb{Z})^r$ that in every coordinate maps z to $2z$, for all $z \in \mathbb{Z}/m\mathbb{Z}$. Note that the norms (M_y) are evaluated modulo $2m$, whereas the (N_x) are evaluated modulo m. Clearly, we have $N_x = M_{2x}$ for all $x \in \mathbb{Z}/m\mathbb{Z}$, so the claim applies. By the first part, the sequence (M_y) has at most $2s$ extremal values; consequently, the same holds for the norm sequence (N_x) of $\mathbf{v}$, and the lemma is proved. ∎

We are now in a position to prove the upper bounds from Theorem 2.6 in the case where $r \leq m$ and r is odd.

PROPOSITION 4.11. *Let r be odd, assume $r \le m$, and let $\mathbf{v} \in V$ be admissible. Then*

$$\|\mathbf{v}\| \le \frac{mr}{4} - \frac{m}{4r}.$$

Proof. Consider the norm sequence $(N_x)_{x\in\mathbb{Z}/m\mathbb{Z}}$ of $\mathbf{v}$. By leaving out all members x of the index set that have $N_{x-1} = N_x$, we arrive at a subsequence $(N'_y)_{y\in\mathbb{Z}/m'\mathbb{Z}}$ of (N_x), with period $m' \le m$. Note that we no longer have $N'_y = \|\mathbf{v} + y\mathbf{e}\|$, because the N'_y have been renumbered. The subsequence has the following properties:

(i) N'_y is a nonnegative integer for all y;
(ii) we have $N'_{y+1} \ne N'_y$ for all y;
(iii) the period m' is equal to m if m is even, and is at least $m - r$ otherwise;
(iv) we have $\|\mathbf{v}\| \le N'_y \le \lfloor mr/2 \rfloor - \|\mathbf{v}\|$ for all y;
(v) the sequence (N'_y) has at most $2r$ extremal values.

The last three of these follow by Lemmas 4.5, 4.8, and 4.10.

Now it is easy to see that if a sequence of integers is squeezed between bounds B from above and A from below and cannot repeat itself, it must have an extremal value at least every $B-A$ elements. Therefore, the number of extremal values times the "band width" $B - A$ provides an upper bound on the length of such a sequence. (With a finite sequence, there are some caveats at the end points, but our sequences are periodic, and hence do not have end points.)

We therefore find

$$\begin{aligned} (2r)(mr/2 - 2\|\mathbf{v}\|) &\ge m' = m && \text{if } m \text{ is even,} \\ (2r)(mr/2 - 1/2 - 2\|\mathbf{v}\|) &\ge m' \ge m - r && \text{if } m \text{ is odd.} \end{aligned}$$

It turns out that the inequalities for the two cases are equivalent. The result follows easily. ∎

Note that the argument could be adapted to yield an upper bound also in the cases where $r > m$. However, the resulting bound $\|\mathbf{v}\| \le mr/4 - 1/4$ is larger than the ones given by Proposition 4.3. For $m = r$, the two bounds coincide.

5. Constructions. After having shown that the values taken by the norm bound function $h(m, r)$ are upper bounds for the norms of admissible vectors, we will now proceed to construct admissible vectors for all m and r, the norm of which actually attains these values. As in the last section, we write $\|\cdot\|$ for the function $\|\cdot\|_2$, as defined in Section 2.

5.1. Even dimension. The case where the dimension r is even is relatively easy. In this case, a useful building block for admissible vectors of

high norm is the *optimal pair*. To achieve flexibility in constructions, we do not require that an optimal pair be itself admissible.

DEFINITION 5.1. An *optimal pair* is a vector $\mathbf{v}$ of length 2 such that for some $x \in \mathbb{Z}/m\mathbb{Z}$, the vector $\mathbf{v} + x\mathbf{e}$ is admissible of maximal norm.

LEMMA 5.2. *If m is even, then for all $y \in \mathbb{Z}/m\mathbb{Z}$, the vector $(y, y + m/2)$ is an optimal pair, and is admissible of norm $m/2$.*

Proof. For all $x \in \mathbb{Z}/m\mathbb{Z}$, we have $\|(y, y+m/2)+(x, x)\| = |y+x|+|y+x+m/2| = m/2$, by Lemma 4.6. This norm is maximal by Proposition 4.3. ∎

LEMMA 5.3. *If m is odd, then for all $y \in \mathbb{Z}/m\mathbb{Z}$ the vector $(y, y + (m-1)/2)$ is an optimal pair. When $y = 0$ or $(m+1)/2 \le \bar{y} \le m-1$, such a vector is admissible of norm $(m-1)/2$.*

Proof. The assertions follow directly from Lemma 4.7, with Proposition 4.3 showing that the attained norm is maximal. ∎

The next result shows that the bounds of Proposition 4.3 are sharp in the case that the dimension r is even.

PROPOSITION 5.4. *Let r be even.*

(i) *If m is even, then there exists an admissible vector $\mathbf{v}$ of length r and norm $mr/4$.*
(ii) *If m is odd, then there exists an admissible vector $\mathbf{v}$ of length r and norm $\lfloor mr/4 - r/4m \rfloor$.*

Proof. For even m, the vector

$$\mathbf{v} = (0, m/2)^{r/2} = (0, m/2, 0, m/2, \ldots, 0, m/2)$$

is clearly admissible of the given norm, by Lemma 5.2 and the fact that the concatenation of admissible vectors yields again an admissible vector.

For the case of odd m, we use Lemma 5.3 and the same fact, with some subtility. Let $\mathbf{v} = (y, y + (m-1)/2)$ be an optimal pair for m, and let $(N_x(v))_{x \in \mathbb{Z}/m\mathbb{Z}}$ be its norm sequence. From Lemma 4.7, it is easy to see that we have

$$N_x(\mathbf{v}) = \begin{cases} (m+1)/2 & \text{if } x \in \{-y+1, -y+2, \ldots, -y+(m-1)/2\}, \\ (m-1)/2 & \text{if } x \in \{-y+(m+1)/2, \ldots, -y+m\}. \end{cases}$$

We will call these two subsets of $\mathbb{Z}/m\mathbb{Z}$ the *high* and *low regions* of $N_x(\mathbf{v})$, respectively.

We will determine $r/2$ optimal pairs such that their concatenation is admissible of maximal norm. For this, it is necessary to select the pairs in such a way that the high regions of their norm sequences are spread as evenly as possible over the total range $x = 0, \ldots, m-1$.

Writing $\mathbf{v}_i = (y_i, y_i + (m-1)/2)$, we take $y_i = -(i-1)(m-1)/2$ for $i \ge 1$. The high region of $(N_x(\mathbf{v}_i))$ starts at $x = (i-1)(m-1)/2+1$ and ends

at $x = i(m-1)/2$. We see that the high regions of $r/2$ pairs, put in a row, cover a contiguous region from $x = 1$ to $x = (r/2)(m-1)/2$; reducing the indices modulo m, we find that every element in the range $x = 0, \dots, m-1$ is covered at least

$$\left\lfloor \frac{\frac{r}{2}\frac{m-1}{2}}{m} \right\rfloor$$

times. Moreover, at $x = 0$, and possibly some elements to the left of $x = 0$, this inequality is an equality, because covering "started" at $x = 1$, strictly to the right of $x = 0$. This means that the concatenation $\mathbf{v}$ of the pairs $\mathbf{v}_i$ thus selected is admissible, and that its norm satisfies

$$\begin{aligned}\|\mathbf{v}\| &\geq \frac{r}{2}\,\frac{m-1}{2} + \left\lfloor \frac{\frac{r}{2}\frac{m-1}{2}}{m} \right\rfloor \\ &= \left\lfloor \frac{r(m-1)}{4} + \frac{r(m-1)}{4m} \right\rfloor = \left\lfloor \frac{mr}{4} - \frac{r}{4m} \right\rfloor.\end{aligned}$$

By Proposition 4.3, we must have equality here, and the construction is finished. ∎

5.2. Odd and small dimension, even modulus. We now proceed to the case of odd dimension, which is more complicated. We first assume that m is even, and that $r < 2m$. The construction of an admissible vector for such parameters is derived from the proof of Proposition 4.11; we try to choose the components of a vector $\mathbf{v} = (v_1, \dots, v_r)$ such that its norm sequence $(N_x(\mathbf{v}))$ has always slope ± 1 and has its extremal values spread as evenly as possible over the range $x = 0, \dots, m-1$. As earlier, we write $V = (\mathbb{Z}/m\mathbb{Z})^r$, and for $x \in \mathbb{Z}/m\mathbb{Z}$, we write $\bar{x}$ for the representative of x in the set $\{0, \dots, m-1\} \subseteq \mathbb{Z}$.

Definition 5.5. Assume m even and r odd. A vector $\mathbf{v} \in V$ satisfying

$$0 = \bar{v}_1 \leq \bar{v}_2 - \frac{m}{2} \leq \bar{v}_3 \leq \bar{v}_4 - \frac{m}{2} \leq \cdots \leq \bar{v}_{r-1} - \frac{m}{2} \leq \bar{v}_r < \frac{m}{2} \tag{5.6}$$

will be called *balanced*.

Lemma 5.7. *Let $\mathbf{v} \in V$ be balanced and let (N_x) be its norm sequence. Then we have $N_{x+1} - N_x = \pm 1$ for all $x \in \mathbb{Z}/m\mathbb{Z}$.*

Proof. As m is even, each individual component v_i has $|v_i + x + 1| - |v_i + x| = \pm 1$ for all x, the sign being positive when $v_i + x = 0, 1, \dots, m/2 - 1$ and negative otherwise. At $x = 0$, we have exactly $(r+1)/2$ "increasing" and $(r-1)/2$ "decreasing" components, so that $N_1 - N_0 = 1$.

But by the alternating arrangement of the v_i around $m/2$, it is clear that after a component changes from increasing to decreasing at a certain x, we cannot have another component doing the same; we must first see a component changing from decreasing to increasing, possibly at the same x

if the corresponding inequality in (5.6) is an equality. Thus, the balance between increasing and decreasing components is always either 1 or -1, and the assertion is clear. ∎

We have shown earlier (Lemma 4.10) that the norm sequence of any vector $\mathbf{v}$ in V has at most $2s$ extremal values, where s is the number of distinct components of $\mathbf{v}$. Now assume $\mathbf{v}$ is balanced. Then in fact, an extremal value will occur whenever the balance between the numbers of increasing and decreasing components of $\mathbf{v}$ changes. For this, we look at the extremal values of the composing sequences. If i is odd, then $0 \le \bar{v}_i < m/2$, so the sequence $|v_i + x|$ has a maximum at $x = m/2 - v_i$. If i is even, then $m/2 \le \bar{v}_i < m$, so a minimum occurs at $x = m - v_i$. All these values for x are possible locations of extremal values in the norm sequence of $\mathbf{v}$. Counting from $x = 1$ onwards, the first location is $m/2 - v_r$, the second is $m - v_{r-1}$, and so on. Finally, we start by having a minimum at $x = 0$.

Thus, let us define

$$m_0 = \|\mathbf{v}\|, \quad m_i = \begin{cases} \|\mathbf{v} + (m/2 - v_{r-i+1})\mathbf{e}\| & \text{if } i \text{ is odd,} \\ \|\mathbf{v} + (m - v_{r-i+1})\mathbf{e}\| & \text{if } i \text{ is even.} \end{cases} \tag{5.8}$$

Then the m_i, for $i = 0, \ldots, r$, include all extremal values of the norm sequence (N_x) of $\mathbf{v}$ in the range $x = 0, \ldots, m/2$.

LEMMA 5.9. *Let* $\mathbf{v}$ *be balanced. Then* $m_1 - m_0 = m/2 - \bar{v}_r$, *while for* $i = 1, \ldots, r-1$,

$$m_{i+1} - m_i = \begin{cases} (\bar{v}_{r-i} - m/2) - \bar{v}_{r-i+1} & \text{if } i \text{ is odd,} \\ (\bar{v}_{r-i+1} - m/2) - \bar{v}_{r-i} & \text{if } i \text{ is even.} \end{cases}$$

Proof. First assume i is odd; then m_i is a possible maximum of the norm sequence, occurring at $x = m/2 - v_{r-i+1}$. The subsequent possible minimum m_{i+1} occurs at $x = m - v_{r-i}$. If these values for x are equal, then we also have $m_{i+1} = m_i$ and the claim is proved. If not, then between these values of x the norm sequence has a constant slope of -1 (cf. Lemma 5.7). Therefore, the difference $m_{i+1} - m_i$, as claimed, is equal to

$$(-1) \cdot ((m - \bar{v}_{r-i}) - (m/2 - \bar{v}_{r-i+1})).$$

The case where $i > 0$ is even and the case $i = 0$ are analogous. ∎

LEMMA 5.10. *Let* $\mathbf{v}$ *be balanced. Then* $\mathbf{v}$ *is admissible if and only if* $N_0 \le m_i \le m_r = mr/2 - N_0$ *for all* i.

Proof. We continue to assume m even and r odd; by definition, we have $m_r = N_{m/2}$. Now we use the symmetry in the norm sequence given by Lemma 4.6, which says that, for all x,

$$N_{x+m/2} = mr/2 - N_x.$$

First assume $\mathbf{v}$ is admissible; then from $N_0 \le N_{x+m/2}$, we find $N_x \le N_{m/2}$ by using the formula twice. Thus in particular all m_i are between N_0 and $m_r = N_{m/2} = mr/2 - N_0$, as claimed.

For the other direction, from $N_0 \le m_i \le m_r$ for all i, we find $N_0 \le N_x \le m_r$ for $x \le m/2$, because the m_i contain all extreme values of the first half of the sequence (N_x). But then by symmetry $N_{x+m/2} = mr/2 - N_x \ge mr/2 - m_r = N_0$, so we have $N_0 \le N_x$ for all x, as desired. ∎

The next lemma shows that there are several equivalent options for the formulation of the norm bound function in (2.4), when m is even and r odd, and r is not too far away from m. In fact, comparable formulae can be given in case m is odd also, but we omit these as they are not needed in what follows. The proof is left to the reader.

LEMMA 5.11. *Let m be even and r odd, and assume $m/2 \le r \le 2m$. Then*

$$\left\lfloor \frac{mr}{4} - \frac{m}{4r} \right\rfloor = \left\lfloor \frac{mr}{4} - \frac{1}{2} \right\rfloor = \left\lfloor \frac{mr}{4} - \frac{r}{4m} \right\rfloor = \begin{cases} mr/4 - 1 & \text{if } m \equiv 0 \pmod 4, \\ mr/4 - 1/2 & \text{if } m \equiv 2 \pmod 4. \end{cases}$$

LEMMA 5.12. *Let m be even and r odd, with $r \le 2m$, and let Q and R be integers such that*

$$m/2 = Qr + R \quad \text{with } 0 \le R < r.$$

Then the quantity $C = mr/2 - 2h(m,r)$ satisfies

$$C = \begin{cases} Q & \text{if } R = 0, \\ Q+1 & \text{if } R \text{ is odd}, \\ Q+2 & \text{if } R \text{ is positive and even.} \end{cases}$$

Furthermore, $C \equiv m/2 \pmod 2$.

Proof. Recall that $h(m,r) = \lfloor mr/4 - m/4r \rfloor$ with our assumptions, by (2.4) and Lemma 5.11. The proof is tedious but easy, and is left to the reader. ∎

PROPOSITION 5.13. *Assume m is even and r is odd, with $r \le 2m$. Then there exists an admissible vector $\mathbf{v} \in V$ of norm $h(m,r) = \lfloor mr/4 - m/4r \rfloor$.*

Proof. We want to construct a balanced vector $\mathbf{v}$ satisfying the requirements. Then by Lemma 5.10, we must choose the components v_i of $\mathbf{v}$ such that the associated quantities m_i satisfy

$$m_0 = h(m,r) \le m_i \le m_r = mr/2 - h(m,r). \tag{5.14}$$

Together with the constraints (5.6), this is an integer programming problem in the variables $\bar{v}_1, \dots, \bar{v}_r$. By Lemma 5.9, the differences $m_{i+1} - m_i$ are, up

to sign and in reverse order, the same as the differences $(\bar{v}_{i+1} - m/2) - \bar{v}_i$ and $\bar{v}_{i+1} - (\bar{v}_i - m/2)$ of the quantities figuring in (5.6). Thus it is enough to specify the values of the m_i, as both m_0 and $v_1 = 0$ are fixed.

An easy but useful corollary of Lemma 5.9, proved using telescoping sums, is that

$$\sum_{i=0}^{r-1} |m_{i+1} - m_i| = m/2 \tag{5.15}$$

(with the usual Euclidean absolute value, because the m_i are integers). Let us write C for the difference $mr/2 - 2h(m,r)$ of the largest and the smallest m_i. By Lemma 5.12, C is equal to or slightly larger than $m/2r$. This observation, together with (5.14), suggests that we take the $|m_{i+1} - m_i|$ all approximately equal to $m/2r$. The rest of the proof will give *exact integer values* for the m_i so as to solve the integer programming problem for the $\bar{v}_i$. We note that, as $m_1 - m_0 = m/2 - \bar{v}_r > 0$ by (5.6), we cannot put $m_1 - m_0 = 0$.

Let Q and R be integers satisfying

$$m/2 = Qr + R \quad \text{with } 0 \le R < r.$$

If $R = 0$, the solution is easy, as we simply put

$$m_{i+1} - m_i = (-1)^i Q \quad \text{for } i = 0, \dots, r-1.$$

By Lemma 5.12, we have $C = Q$ in this case, so that (5.14) is satisfied.

If $R \neq 0$, we put

$$m_{i+1} - m_i = \begin{cases} (-1)^i (Q+1) & \text{for } i = 0 \text{ and } i = r-R+1, \dots, r-1, \\ (-1)^i Q & \text{for } i = 1, \dots, r-R. \end{cases}$$

If R is then odd, this implies that $m_i = m_0 + 1$ for all even i with $2 \le i \le r - R$, and $m_i = m_0$ for the other even i; furthermore, by Lemma 5.12 we have $C = Q + 1$, and in fact $m_r = m_0 + C$, as the number of i with $|m_{i+1} - m_i| = Q$, which is $r - R$, is even. If R is even and positive, we have $m_i = m_0 + 1$ for all even $i \ge 2$. In this case, by Lemma 5.12 we have $C = Q + 2$, and in fact we get $m_r = m_0 + Q + 2$, as the number of steps of size Q is then odd.

It follows that the integer programming problem defining the $\bar{v}_i$ always has a solution, so that the existence of the required vector is proved. ∎

5.3. Odd dimension, odd modulus. We continue to assume that r is odd. We will now reduce the case of odd modulus m to the even case, using *division by* 2; this seems to be the easiest way of extending the argument used in the proof of Proposition 5.13. For $r \le m$, we achieve this reduction in Corollary 5.20 below. The case $r > m$ will be dealt with in Section 5.4.

The group homomorphism $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/2m\mathbb{Z}$ sending 1 to 2 induces a linear map $\mu_2 : (\mathbb{Z}/m\mathbb{Z})^r \to (\mathbb{Z}/2m\mathbb{Z})^r$ that multiplies all components by 2. The image of μ_2 consists of those vectors in $(\mathbb{Z}/2m\mathbb{Z})^r$ that have all their components even; we will call these *even vectors*. The map μ_2 has an inverse on the set of even vectors that we shall call *division by* 2 and denote by $\mathbf{v} \mapsto \mathbf{v}/2$.

Note that $\|\mu_2(\mathbf{v})\|$, as evaluated in $(\mathbb{Z}/2m\mathbb{Z})^r$, is equal to $2\|\mathbf{v}\|$, when evaluated in $(\mathbb{Z}/m\mathbb{Z})^r$, so that the Lee norm is multiplied by 2 under the map μ_2; likewise, division by 2 halves the norm.

LEMMA 5.16. *If $\mathbf{v} \in (\mathbb{Z}/2m\mathbb{Z})^r$ is even and admissible, then $\mathbf{v}/2 \in (\mathbb{Z}/m\mathbb{Z})^r$ is also admissible.*

Proof. We have $\|\mathbf{v}\| \le \|\mathbf{v} + x\mathbf{e}\|$ for all $x \in \mathbb{Z}/2m\mathbb{Z}$; in particular, this holds for all *even* $x \in \mathbb{Z}/2m\mathbb{Z}$, and hence $\|\mathbf{v}/2\| \le \|\mathbf{v}/2 + x\mathbf{e}\|$ for all $x \in \mathbb{Z}/m\mathbb{Z}$. ∎

Recall that $h(m, r)$, as defined in (2.4), gives the maximal norm of an admissible vector of length r and modulus m.

LEMMA 5.17. *Let $m \equiv 2$ modulo 4, and assume $r < 2m$ and r odd. Then*

$$h(m/2, r) = \lfloor h(m, r)/2 \rfloor.$$

Furthermore, if Q and R are integers such that $m/2 = Qr + R$ with $0 \le R < r$, then $h(m, r)$ is even if $R = 0$ or $R \equiv 2 \pmod 4$ or $R \equiv r \pmod 4$, and odd otherwise.

Proof. We use Lemma 5.11 to extend the formula $h(m, r) = \lfloor mr/4 - m/4r \rfloor$ from (2.4), which holds for $r \le m$, to the range $m < r < 2m$.

Now we have $h(m/2, r) = \lfloor mr/8 - m/8r \rfloor$ and $h(m, r) = \lfloor mr/4 - m/4r \rfloor$. Because $\lfloor x/2 \rfloor = \lfloor \lfloor x \rfloor /2 \rfloor$ for any real $x \ge 0$, the first assertion easily follows.

We now prove the second assertion. By substituting $2(Qr + R)$ for m in the formula for $h(m, r)$, we find

$$h(m, r) = Q \cdot \frac{r^2 - 1}{2} + \begin{cases} 0 & \text{if } R = 0, \\ (Rr - 2)/2 & \text{if } R \text{ is nonzero and even}, \\ (Rr - 1)/2 & \text{if } R \text{ is odd}. \end{cases}$$

The first term is even, so the parity of $h(m, r)$ equals the parity of the second term. ∎

PROPOSITION 5.18. *Let m be congruent to 2 modulo 4, and assume $r \le m/2$ and r odd. Then there exists in V an* even *admissible vector of norm $2h(m/2, r)$.*

Proof. We will use the method developed in the proof of Proposition 5.13 to construct a balanced admissible *even* vector $\mathbf{v}$ satisfying the requirements.

As above, we consider the components v_i of $\mathbf{v}$ as the variables of an integer programming problem, which is here given by the constraints (5.6), together with the following adaption of (5.14):

$$m_0 = 2h(m/2, r) \leq m_i \leq m_r = mr/2 - 2h(m/2, r) \tag{5.19}$$

for $i = 0, \ldots, r$, and the additional constraint that all the v_i must be even. Of course, as we fix $v_1 = 0$ and as $m/2$ is odd, this is equivalent to all the differences $(\bar{v}_{i+1} - m/2) - \bar{v}_i$ or $\bar{v}_{i+1} - (\bar{v}_i - m/2)$ being *odd*, and this in turn to the differences $m_{i+1} - m_i$ being odd for all i (cf. Lemma 5.9).

Write C' for the difference $m_r - m_0 = mr/2 - 4h(m/2, r)$, and let C be as in Lemma 5.12. By Lemma 5.17, we see that (5.14) is equivalent to (5.19), and we have $C' = C$, whenever $h(m, r)$ is even; if $h(m, r)$ is odd, this means that an even vector of norm $h(m, r)$ does not exist, and we have to weaken (5.14), taking $C' = C + 2$.

As before, let Q and R be integers satisfying

$$m/2 = Qr + R \quad \text{with } 0 \leq R < r.$$

We now have the same three cases, depending on whether R is zero, odd, or nonzero and even. Again, we recall that we may not put $m_1 - m_0 = 0$.

First, suppose $R = 0$. As $C = C'$ in this case, we have the same constraints as in the proof of Proposition 5.13. There, we gave $|m_{i+1} - m_i|$ the value Q for all i. But Q is odd, which means that we automatically obtain an even vector, and we are done.

Now suppose R is odd. We must distinguish two subcases. Thus, first suppose that R and r are congruent modulo 4. It then follows by Lemma 5.17 that $C' = C = Q + 1$. We cannot give $|m_{i+1} - m_i|$ the value Q now, as we did previously, since Q is even. Instead, we take

$$m_{i+1} - m_i = \begin{cases} (-1)^i(Q+1) & \text{for } i = 0, \ldots, (r+R)/2 - 1, \\ (-1)^i(Q-1) & \text{for } i = (r+R)/2, \ldots, r-1. \end{cases}$$

Note that by the assumption $r \leq m/2$, we have $Q \geq 1$. Here we have $m_i = m_0$ for even $i \leq (r + R)/2$ and $m_i = m_0 + 2$ for larger even i.

If R is odd, but not congruent to r modulo 4, we find by Lemma 5.17 that $h(m, r)$ is odd, and we have to take $C' = C+2 = Q+3$. The assignment of values will be

$$m_{i+1} - m_i = \begin{cases} (-1)^i(Q+1) & \text{for } i = 0, \ldots, (r+R)/2 - 2, \\ (-1)^i(Q-1) & \text{for } i = (r+R)/2 - 1, \ldots, r-2, \\ Q+3 & \text{for } i = r-1. \end{cases}$$

Finally, suppose R is nonzero and even. Again we find two subcases. Assume $R \equiv 2 \pmod 4$; then by Lemma 5.17 we find $C' = C = Q + 2$. As we cannot assign the even value of $Q + 1$, we take the assignment of values

to be

$$m_{i+1} - m_i = \begin{cases} (-1)^i Q & \text{for } i = 0, \dots, r - R/2 - 1, \\ (-1)^i (Q+2) & \text{for } i = r - R/2, \dots, r - 1. \end{cases}$$

The last case is where R is nonzero and $R \equiv 0 \pmod 4$. By Lemma 5.17, we see that $h(m,r)$ is odd and we must allow $C' = C + 2 = Q + 4$ in (5.19) in order for an even vector to exist. Here, one can assign values as follows:

$$m_{i+1} - m_i = \begin{cases} (-1)^i Q & \text{for } i = 0, \dots, r - 2 - (R-4)/2, \\ (-1)^i (Q+2) & \text{for } i = r - 1 - (R-4)/2, \dots, r - 2, \\ Q + 4 & \text{for } i = r - 1. \end{cases}$$

In all the preceding cases, one checks easily that (5.19) is satisfied; the checks are the easier as we have chosen values for the m_i such that $m_i = m_0$ for all even i, except when $R \equiv r \pmod 4$. ∎

COROLLARY 5.20. *Let m be odd, and assume $r \le m$ and r odd. Then there exists in V an admissible vector of norm $h(m,r)$.*

Proof. Let $\mathbf{v}$ be an admissible even vector in $(\mathbb{Z}/2m\mathbb{Z})^r$ of norm $2h(m,r)$, as provided by Proposition 5.18; then $\mathbf{v}/2$ is the desired vector in V. ∎

5.4. Large, odd dimension. We just proved the norm bounds of Theorem 2.6 sharp for r odd and at most equal to $2m$ (for m even) or at most equal to m (for m odd). The last step of the proof of the theorem is to reduce the case of arbitrarily large odd dimension to one of these cases, or to the case of even r. For this, we use the fact that admissible vectors of maximal norm are particularly easy to construct when the dimension r is *divisible* by the modulus m.

LEMMA 5.21. *Suppose m divides r. Then the vector*

$$(0, 1, \dots, m-1)$$

is admissible of maximal norm $m^2/4$ (if m is even), resp. $(m^2-1)/4$ (if m is odd).

Proof. Let $\mathbf{v} = (0, 1, \dots, m-1)$; adding $\mathbf{e} = (1, \dots, 1)$ to the vector only permutes the coordinates, so $\mathbf{v}$ is clearly admissible. Its norm is given by Lemma 4.1. ∎

LEMMA 5.22. *Suppose $\mathbf{v}$ is an admissible vector of length r and maximal norm. If $r \ge m$, then the concatenation of $\mathbf{v}$ with $(0, 1, \dots, m-1)$, of length $r + m$, is also admissible of maximal norm. If m is odd and r is even, this even holds for all $r \ge 1$.*

Proof. Write $\mathbf{w}$ for the concatenation of $\mathbf{v}$ with $(0, 1, \dots, m-1)$. We use the fact that the concatenation of two admissible vectors is admissible, with the norm of the concatenated vector being the sum of the norms of the

summands. Therefore, it remains to prove that the concatenation again has maximal norm.

According to Proposition 4.3, there are three cases. Now the equalities

$$\frac{mr}{4} + \frac{m^2}{4} = \frac{m(r+m)}{4},$$
$$\left\lfloor \frac{mr}{4} - \frac{1}{2} \right\rfloor + \frac{m^2}{4} = \left\lfloor \frac{m(r+m)}{4} - \frac{1}{2} \right\rfloor,$$
$$\left\lfloor \frac{mr}{4} - \frac{r}{4m} \right\rfloor + \frac{m^2-1}{4} = \left\lfloor \frac{m(r+m)}{4} - \frac{r+m}{4m} \right\rfloor$$

settle the cases of m and r both even, m even and r odd, and m odd, respectively. ∎

PROPOSITION 5.23. *Let m be given. If the norm bounds given in Theorem 2.6 are sharp for r with $1 \le r \le 2m-1$, then they are sharp for all r. If the norm bounds are sharp for m odd and r even with $r \le m$, then they are also sharp for r odd with $m < r \le 2m-1$.*

Proof. Suppose we have m and r with $r \ge 2m$; write $r = Qm + R$ with integers Q, R satisfying $m \le R < 2m$. An admissible vector of maximal norm of length r is constructed by concatenating such a vector of length R with Q copies of $(0, 1, \ldots, m-1)$, by Lemma 5.22.

As to the second statement, let m and r be odd with $m < r \le 2m-1$, and let $\mathbf{v}$ be an admissible vector of length $r-m$ and maximal norm. Then by the last statement of Lemma 5.22, the concatenation of $\mathbf{v}$ with $(0, 1, \ldots, m-1)$ is admissible of length r and maximal norm. ∎

6. Proof of Theorems 2.6, 1.2, and 1.3

Proof of Theorem 2.6. Write $V = (\mathbb{Z}/m\mathbb{Z})^r$, as before, and let $\|\cdot\|$ denote the norm $\|\cdot\|_2$, as defined in Section 2. We must prove that for all m and r, admissible vectors of norm $h(m,r)$ exist in V, and that admissible vectors cannot have higher norms.

The fact that $h(m,r)$ forms an upper bound for the norm of an admissible vector is proved in Propositions 4.3, for the cases where $r \ge m$ or r is even, and 4.11, for the cases where r is odd and $r \le m$. In fact, if $r \le m$ and m and r both odd, it is clear that

$$\frac{mr}{4} - \frac{r}{4m} \ge \frac{mr}{4} - \frac{m}{4r};$$

here the left hand side is the bound given by Proposition 4.3, and the right hand is given by Proposition 4.11. Also, if m is even and r odd, then for $r \le m/2$ the inequality

$$\frac{mr}{4} - \frac{1}{2} \ge \frac{mr}{4} - \frac{m}{4r}$$

shows that the left bound, given by Proposition 4.3, is larger than the right one from Proposition 4.11, while for $m/2 < r \leq m$ the floors of the two bounds are shown to be equal by Lemma 5.11.

The question whether the norm bound $h(m,r)$ is sharp was settled in Section 5, in several cases, as follows.

For r even, concrete vectors attaining the norm bound are given by Proposition 5.4.

Assume r is odd. By Proposition 5.23, we may reduce to a case with $r < 2m$, where the new r can have either parity. Now if r is even, we use Proposition 5.4 to conclude the argument. If r is odd and m is even, we use Proposition 5.13. If both m and r are odd and $m < r < 2m$, we use the second statement of Proposition 5.23 to conclude: the norm bound is sharp for modulus m and even dimension $r-m$ by Proposition 5.4, and hence it is sharp for modulus m and odd dimension r. If, finally, both m and r are odd and $r \leq m$, we conclude using Corollary 5.20. ∎

We can now prove our results on Waring's problem.

Proof of Theorem 1.2. Note that the nonzero $((p^{r-1}-1)/r)$th powers in $\mathbb{F}_{p^{r-1}}$ are exactly the rth roots of unity.

Now let ξ be a primitive rth root of unity in $\mathbb{F}_{p^{r-1}}$. Since p is a primitive root modulo r, the field $\mathbb{F}_{p^{r-1}}$ is generated by ξ, i.e. $\{1, \xi, \dots, \xi^{r-2}\}$ is a basis of $\mathbb{F}_{p^{r-1}}$ over $\mathbb{F}_p$. Since

$$\sum_{i=0}^{r-1} \xi^i = 0$$

is the sole relation between the ξ^i, we can consider $\mathbb{F}_{p^{r-1}}$ as the $\mathbb{F}_p$-module V, as above, with the generators $1, \xi, \dots, \xi^{r-1}$, and an expression (1.1) of an element a as sum of powers with as few terms as possible corresponds to an admissible coordinate vector for a, as an element of V. We now look for the worst such vectors in terms of the norm $\|\cdot\|_1$.

Thus, as $\gcd(p,r) = 1$, the result follows by Theorem 2.5. ∎

Proof of Theorem 1.3. The nonzero $((p^{r-1}-1)/(2r))$th powers in $\mathbb{F}_{p^{r-1}}$ are exactly the $(2r)$th roots of unity in $\mathbb{F}_{p^{r-1}}$, and again $\mathbb{F}_{p^{r-1}}$ is generated by a primitive rth root of unity. We consider the same module V as in the proof of Theorem 1.2. Now, a representation of the form (1.1) with a minimal number of terms corresponds to an expression

$$a = \sum_{i=0}^{r-1} \pm v_i \xi^i,$$

with $\sum |v_i|$ minimal; but this is the same as having

$$\|(\pm v_0, \dots, \pm v_{r-1})\|_2$$

minimal, where by the linear dependence of the ξ^i we may add $\mathbf{e} = (1, \ldots, 1)$ if that reduces the norm. The problem is thus to characterise admissible vectors of maximal norm for the norm $\|\cdot\|_2$. But this is done in Theorem 2.6. ∎

Acknowledgements. We want to thank Hendrik Lenstra for suggesting this way of attacking Waring's problem.

The research that led to this publication was supported by the Austrian Science Foundation FWF, in Linz by Projects S8313 and P19004-N18, and in Graz by Project S9606, which is part of the Austrian National Research Network "Analytic Combinatorics and Probabilistic Number Theory".

References

[1] E. R. Berlekamp, *Algebraic Coding Theory*, McGraw-Hill, New York, 1968.
[2] R. A. Brualdi, S. Litsyn, and V. S. Pless, *Covering radius*, in: Handbook of Coding Theory, North-Holland, Amsterdam, 1998, 755–826.
[3] G. D. Cohen, I. S. Honkala, S. Litsyn, and A. Lobstein, *Covering Codes*, Elsevier, Amsterdam, 1997.
[4] C. Garcia and P. Solé, *Diameter lower bounds for Waring graphs and multiloop networks*, Discrete Math. 111 (1993), 257–261.
[5] T. Helleseth, *On the covering radius of cyclic linear codes and arithmetic codes*, Discrete Appl. Math. 11 (1985), 157–173.
[6] C. Small, *Diagonal equations over large finite fields*, Canad. J. Math. 36 (1984), 249–262.
[7] A. Weil, *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc. 55 (1949), 497–508.
[8] A. Winterhof, *On Waring's problem in finite fields*, Acta Arith. 87 (1998), 171–177.
[9] —, *A note on Waring's problem in finite fields*, ibid. 96 (2001), 365–368.
[10] C. E. van de Woestijne, Implementation of the results of the present paper in KASH 2.x, http://www.opt.math.tugraz.at/~cvdwoest/maths/leenorm.kash.

Arne Winterhof
Johann Radon Institute for
Computational and Applied Mathematics
Austrian Academy of Sciences
Altenbergerstraße 69
4040 Linz, Austria
E-mail: arne.winterhof@oeaw.ac.at

Christiaan van de Woestijne
Institut für Mathematik B
Technische Universität Graz
Steyrergasse 30
8010 Graz, Austria
E-mail: c.vandewoestijne@tugraz.at

Received on 8.10.2008
and in revised form on 21.7.2009 (5820)