comput complexity **1** (1991), 360–394 1016-3328/91/040360-35 $1.50+0.20

EFFICIENT AND OPTIMAL EXPONENTIATION IN FINITE FIELDS

JOACHIM VON ZUR GATHEN

Abstract. Optimal sequential and parallel algorithms for exponentiation in a finite field containing F_q are presented, assuming that qth powers can be computed for free.
Subject classifications. 68Q40; 11Y16, 12Y05.

1. Introduction

In this paper, we study the complexity of exponentiation in finite fields. This problem is important in some cryptographic applications, and has been considered for fields F_{2^n}. In a specific structured model, appropriate for the problem, we derive asymptotically optimal sequential algorithms, and (exactly) optimal parallel algorithms.

Let us first describe the model. We consider exponentiation in a finite field F_{q^n} with q^n elements, where q is a prime power and $n \geq 1$. Suppose that $(\beta_0, \ldots, \beta_{n-1})$ is a *normal basis* of F_{q^n} over a field F_q with q elements, so that $\beta_i = \beta_0^{q^i}$ for all i. An arbitrary element a of F_{q^n} can be uniquely written as $a = \sum_{0 \leq i < n} a_i \beta_i$ with $a_0, \ldots, a_{n-1} \in \mathsf{F}_q$. For any $j \in \mathsf{N}$, we have

$$a^{q^j} = \sum_{0 \leq i < n} a_i \beta_i^{q^j} = \sum_{0 \leq i < n} a_i \beta_{i+j} \,,$$

with index arithmetic modulo n. Thus taking qth powers amounts to a cyclic shift of coordinates. This may be much less expensive than a general multiplication. A basic assumption for our algorithms is that *computing qth powers is for free.*

This assumption can be justified in several ways:

- In a normal basis qth powers correspond to a cyclic shift; in this form, the assumption occurs in the literature for $q = 2$ (Beth *et al.* 1986, Wang *et al.* 1987, Agnew *et al.* 1988, Stinson 1990). We note that normal bases are easy to find (see von zur Gathen & Giesbrecht 1990 and the literature given there).

- In an arbitrary basis $\alpha_0, \ldots, \alpha_{n-1}$ for F_{q^n} over F_q, a table with the n^2 entries $\alpha_i^{q^j}$, for $0 \leq i, j < n$, might be precomputed. Then qth powers can be calculated with a table look-up and linear operations. (Here, as in the previous point, we think of an element of F_{q^n} as being represented by its coordinates in the given basis.)

- The multiplication of two input-dependent values is often considered to be more costly than a *scalar* operation, such as multiplication of an input-dependent value by a constant, or an addition. In fact, the successful *non-scalar model* assumes all scalar operations are free. Now qth powers can be computed with only scalar operations.

- Without some assumption of this type, no good parallel algorithms are possible, with parallel time $(\log n)^{O(1)}$. Our algorithms are arithmetic circuits over F_{q^n}, using arithmetic operations (in fact, mainly multiplication) in F_{q^n}. But any arithmetic circuit for powers in F_{q^n} has depth at least $n/3$ (von zur Gathen 1987, von zur Gathen & Seroussi 1991), if every operation is counted.

Thus we take as an appropriate model for the exponentiation problem *arithmetic circuits* over F_{q^n} (using instructions $+, -, *, /$) with free qth powers. Note that we have motivated the assumption of free qth powers by considering "low-level" computations over F_q, but that in the sequel we will only speak in the "high-level language" of computing over F_{q^n}.

Section 2 presents an algorithm using *size* (= total number of multiplications) about $n/\log_q n$ and *depth* (= parallel time) about $\log_2 n$. (Size n with depth $\log_2 n$ is trivial.) For $q = 2$, this is a slight improvement of Stinson's (1990) result of about $\frac{3}{2} n/\log_2 n$.

In Section 3, a counting argument shows that the size cannot be improved below essentially $\frac{1}{3} n/\log_q n$. This holds for circuits using $+, -, *$, or using $*, /$; when all four operations are used, it has to be assumed that the circuit is *defined* at sufficiently many inputs. (The algorithm actually uses only $*$.)

Starting in Section 4, we consider the depth in detail, and prove sharp results. We introduce "addition chains with free multiples by q", which corre-

spond to "multiplication with free qth powers", and analogous "addition/subtraction chains". In both models, we determine *exactly* the parallel complexity of some $e \in \mathbf{N}$, in terms of the "sum of digits" $\sigma_q(e)$ in q-ary representation for addition chains (namely, $\lceil \log_2 \sigma(e) \rceil$), and in terms of a similar invariant $\sigma_q^{\pm}(e)$ for addition/subtraction chains (namely, $\lceil \log_2^{\pm} \sigma(e) \rceil$), based on a "signed-digit representation".

For $q = 2$, this signed-digit representation is discussed at length in Reitwiesner (1960) who gives an algorithm to compute $\sigma_2^{\pm}(e)$ and an optimal representation. The use of divisions for a related problem, namely modular exponentiation, was suggested by Jedwab & Mitchell (1989), and they show how to find $\sigma_2^{\pm}(e)$ and an optimal representation of e (for $q = 2$). Lengauer & Mehlhorn (1986) and Takagi *et al.* (1985) use a redundant binary representation, with digits $-1, 0, 1$, to construct binary addition and multiplication algorithms for VLSI implementation.

Section 5 provides an efficient way to calculate $\sigma_q^{\pm}(e)$ from e, and also an optimal parallel algorithm. This is technically the most challenging part of the paper (Theorem 5.4). Section 6 determines the maximal value of $\sigma_q^{\pm}(e)$. In the last section, Fermat's Little Theorem provides a small surprise: it may be more efficient to compute the power $e + s(q^n - 1)$ rather than e, for some small s; by Fermat's Theorem, these take the same value.

2. Multiplication and free powers

We consider a standard model for algebraic computation: *arithmetic circuits* (or *straight-line programs*), which have input gates, constant gates, and gates for the addition, subtraction, multiplication, or division of two field elements. We only use multiplication in this section. The *depth* (= parallel time = delay) is the maximal length (= number of gates) of paths in such a circuit, and the *size* (= total work) is the number of gates. We can stratify the circuit into levels, with input and constant gates at level zero, and otherwise a gate at higher level than any of its two inputs; the number of the highest level equals the depth. Then the *width* (= number of processors) of a circuit is the maximal number of gates at any level. Trivially, we have

$$\text{width} \leq \text{size} \leq \text{depth} \cdot \text{width}. \tag{2.1}$$

A basic assumption for our algorithms is that qth powers are free.

Since $a^{q^n} = a$ for all $a \in \mathbf{F}_{q^n}$, by Fermat's Little Theorem, we may assume that our exponent e satisfies $0 \leq e < q^n$. We take the *q-ary representation* of e

$$e = \sum_{0 \leq i < n} e_i q^i \text{ with } 0 \leq e_0, \ldots, e_{n-1} < q.$$

Then x^e can obviously be computed as follows:

ALGORITHM 1.

1. For $2 \leq j < q$, compute x^j,
2. For $1 \leq i < n$, compute $y_i = (x^{e_i})^{q^i}$,
3. Return $x^e = \prod_{0 \leq i < n} y_i$.

Using a binary tree of multiplications (executed from root to leaves) in step 1 leads to depth $\delta = \lceil \log_2(q-1) \rceil$, width $\max\{2^{\delta-2}, q-1-2^{\delta-1}\}$, and size $q-2$. (For $q = 2$, the width is 0.) Step 2 is free. A binary tree of multiplications (executed from leaves to root) in step 3 yields depth $\lceil \log_2 n \rceil$, width $\lfloor n/2 \rfloor$, and size $n-1$.

Thus we have the following result.

THEOREM 2.1. *Let $0 \leq e < q^n$. Then $x^e \in \mathbf{F}_{q^n}[x]$ can be computed in depth $\delta + \lceil \log_2 n \rceil$, width $\max\{2^{\delta-2}, q-1-2^{\delta-1}, \lfloor n/2 \rfloor\}$, and size $q+n-3$, where $\delta = \lceil \log_2(q-1) \rceil$.*

The idea of the next algorithm is that short *patterns* might occur repeatedly in the q-ary representation of e, and that precomputation of all such patterns might lower the overall cost. This idea is useful for "addition chains" (see Knuth 1982, 4.6.3, and the references given there) and for "word chains" (Berstel & Brlek 1989), and has been applied to our exponentiation problem in characteristic two by Agnew *et al.* (1988) and Stinson (1990). The algorithm below answers positively the question about general q, in the last sentence of Stinson's paper.

We choose some pattern length $r \geq 1$, set $s = \lceil n/r \rceil$, and write $e = \sum_{0 \leq i < s} b_i q^{ri}$ with $0 \leq b_i < q^r$ for all i.

ALGORITHM 2.

1. Compute all x^d for $2 \leq d < q$.
2. Compute all x^d for $q < d < q^r$.
3. For $0 \leq i < s$, compute $y_i = (x^{b_i})^{q^{ri}}$.

4. Return $x^e = \prod_{0 \le i < s} y_i$.

The cost of step 1 has been given above. We implement step 2 in $\lceil \log_2 r \rceil$ stages $1, \ldots, \lceil \log_2 r \rceil$ as follows. For any $d \in \mathbf{N}$ with q-ary representation $d = \sum_i d_i q^i$, let

$$w(d) = \#\{i : d_i \neq 0\} \tag{2.2}$$

be the q-ary *Hamming weight* of d. In stage i, we compute all x^d (not previously computed) with $q < d < q^r$, $d \not\equiv 0 \bmod q$, and $w(d) \le 2^i$. Each new d in stage i is of the form $d = d_1 + q^j d_2$, for some $j \ge 1$ and d_1, d_2 computed before stage i. Then

$$x^d = x^{d_1} \cdot (x^{d_2})^{q^j},$$

and each stage $1, \ldots, \lceil \log_2 r \rceil$ can be performed in depth 1.

After the last stage, we have all required powers for $d \not\equiv 0 \bmod q$; the ones with $d \equiv 0 \bmod q$ can be computed free of charge. There are exactly $q^r - q^{r-1} - 1$ integers d with $2 \le d < q^r$ and $d \not\equiv 0 \bmod q$. Since each multiplication yields a new x^d, the total size for steps 1 and 2 is $(q-1)q^{r-1} - 1$. This also bounds the width.

Since step 3 is free, and we can use a binary multiplication tree in step 4, we have the following.

THEOREM 2.2. *Let $0 \le e < q^n$, $1 \le r$ and $s = \lceil n/r \rceil$. Then $x^e \in \mathsf{F}_{q^n}[x]$ can be computed by multiplications and free qth powers in depth $\lceil \log_2(q-1) \rceil + \lceil \log_2 r \rceil + \lceil \log_2 s \rceil$, width $\max\{(q-1)q^{r-1} - 1, \lfloor s/2 \rfloor\}$, and size $(q-1)q^{r-1} + s - 2$.*

For any $r, t \in \mathbf{N}$ with $n/r \le 2^t$, we also have $s = \lceil n/r \rceil \le 2^t$, and thus $\lceil \log_2 s \rceil = \lceil \log_2(n/r) \rceil$. If $\lambda = \lceil \log_2 r \rceil$, then $2^{\lambda-1} < r \le 2^\lambda$ and $n/r < n/2^{\lambda-1}$. Thus $\log_2(n/r) < \log_2 n - (\lambda - 1)$, and $\lceil \log_2 s \rceil \le \lceil \log_2 n \rceil - \lambda + 1$. For any choice of r we have

$$\lceil \log_2 n \rceil \le \lceil \log_2 r \rceil + \lceil \log_2 s \rceil \le \lceil \log_2 n \rceil + 1. \tag{2.3}$$

We give two applications of the theorem. The goal in the first application is to minimize the size (and Corollary 3.3 below shows that the result is asymptotically optimal for large n up to a factor of three), and the goal in the second application is to minimize the depth.

COROLLARY 2.3. *Let q be a prime power, $n \ge q^5$, $0 \le e < q^n$, and either $q \ge 3$ or $n \ge 626$. Then $x^e \in \mathsf{F}_{q^n}[x]$ can be calculated by multiplications and free qth powers with the following costs:*

(i) depth $\lceil \log_2 qn \rceil + 2$, *width less than* $\frac{n}{2\log_q n}(1+\epsilon)$, *and size less than* $\frac{n}{\log_q n}(1+\epsilon)$, *where* $\epsilon = (10\log_q \log_q n + 6)/\log_q n$.

(ii) depth $\lceil \log_2(q-1) \rceil + \lceil \log_2 n \rceil$, *width less than* $\frac{n}{\log_q n}(1+\epsilon)$, *and size less than* $\frac{2n}{\log_q n}(1+\epsilon)$.

PROOF. (i) We apply Theorem 2.2 with $r = \lfloor \log_q n - 2\log_q \log_q n \rfloor$. Then, using (2.3), the depth is at most

$$\lceil \log_2(q-1) \rceil + \lceil \log_2 n \rceil + 1 \leq \lceil \log_2 qn \rceil + 2.$$

Furthermore,

$$\begin{aligned} (q-1)q^{r-1} &\leq (q-1)q^{\log_q n - 2\log_q \log_q n - 1} < \frac{n}{(\log_q n)^2}, \qquad (2.4) \\ s-1 &\leq \frac{n}{r} < \frac{n}{\log_q n - 2\log_q \log_q n - 1}. \end{aligned}$$

We first assume that $q \geq 3$. Suppose that $u, v \in \mathbf{R}$ are such that $u, v \geq 1$ and

$$\frac{2\log_3 z + 1}{z} \leq \frac{u-1}{u} \text{ for all real } z \geq v. \qquad (2.5)$$

We then have $\log_q z \leq \log_3 z$, and

$$\left(1 - \frac{2\log_q z + 1}{z}\right)^{-1} \leq 1 + u \cdot \frac{2\log_q z + 1}{z}$$

for $z \geq v$, and hence for $n \geq q^v$ we have

$$\frac{\log_q n}{\log_q n - 2\log_q \log_q n - 1} \leq 1 + u \cdot \frac{2\log_q \log_q n + 1}{\log_q n},$$

$$s - 1 < \frac{n}{\log_q n}\left(1 + \frac{2u\log_q \log_q n + u}{\log_q n}\right).$$

One checks that $u = v = 5$ satisfies (2.5). This and (2.4) imply the size estimate, and the width bound follows from

$$1 \leq \frac{n}{\log_q n} \cdot \frac{5 \cdot 0.2}{\log_q n},$$

$$\left\lfloor \frac{s}{2} \right\rfloor \leq \frac{1}{2}((s-1)+1) < \frac{1}{2} \cdot \frac{n}{\log_q n} \cdot \left(1 + \frac{10 \log_q \log_q n + 5 \cdot 1.2}{\log_q n}\right).$$

This proves (i) for $q \geq 3$. If we replace $\log_3$ in (2.5) by $\log_2$, then the condition holds for $u = 5$ and $v = 9.289$, and (i) follows for $q = 2$ and $n \geq 626$.

(ii) We let $r_2 = 2^\lambda$ be the largest power of 2 not larger than $r = \lfloor \log_q n - 2 \log_q \log_q n \rfloor$, and $s_2 = \lceil n/r_2 \rceil$. Then $r_2 \leq r$ and $\lceil \log_2 r_2 \rceil + \lceil \log_2 s_2 \rceil = \lceil \log_2 n \rceil$. Furthermore, $n/r_2 < 2n/r$, and thus $s_2 \leq 2s$ and $\lfloor s_2/2 \rfloor \leq 2 \cdot s/2$. The claim now follows using the estimates from (i). □

For small values of n, the theorem will yield similar results, but with different constants. In this paper, we study the size and depth for exponentiation in detail; the width is considered in von zur Gathen (1992).

3. A lower bound on size

A counting argument will now prove lower bounds on the size required for exponentiation, asymptotically matching the upper bounds from Section 2. We first have to describe in more detail the models of computation that we will consider. First recall *arithmetic circuits* (or *straight-line programs*), the standard model for computation over a field F, as at the beginning of Section 2. Such a circuit α has input gates whose values are indeterminates $x_1, \ldots, x_n$, constant gates with values from a field F, and gates for addition, subtraction, multiplication, and division of previously computed values. At each gate v of such a circuit α, a rational function $f_v \in F(x_1, \ldots, x_n)$ is computed. A condition is that no division by the rational function zero occurs. The *size* of α is the total number of arithmetic gates $+, -, *, /$ in α.

For our purposes the following variant of arithmetic circuits is appropriate. We have $n = 1$, only one input gate v_0 with $f_{v_0} = x = x_1$, a set $\Gamma \subseteq F$ of constants, and only one special output gate v_ℓ, where ℓ is the size of α. At each gate v,

$$f_v = (f_{w_1})^{q^{e_1}} \circ (f_{w_2})^{q^{e_2}} \in F(x) \tag{3.1}$$

is computed, where $\circ \in \{+, -, *, /\}$ is an operation, f_{w_1} and f_{w_2} are previously computed results or constants from Γ, and $e_1, e_2 \in \mathbf{N}$. We call such a circuit an *arithmetic circuit with free qth powers*. It *computes* x^e if there exists $d \in \mathbf{N}$ such that $f_{v_\ell}^{q^d} = x^e$. We note that the only slightly unnatural constraint is the

restriction we will impose on the constants; all algorithms in Sections 2 have $\Gamma = \emptyset$.

We denote by $\pi_F^e : F \to F$ the exponentiation function, with $\pi_F^e(a) = a^e$. A circuit α as above *value-computes* π_F^e if there exists $d \in \mathbf{N}$ such that for any $a \in F$ in the execution of α under the substitution $x \leftarrow a$, either a division by zero occurs (then α is *undefined* at a) or $f_{v_\ell}(a)^{q^d} = a^e$ (and α is *defined* at a). If α computes x^e, then α also value-computes $\pi_F^e(a)$; the reverse implication is true over infinite fields, but may fail over finite fields. This is discussed in Section 7. "Value-computing" is a rather weak notion, and hence appropriate for lower bounds, but not necessarily for upper bounds.

THEOREM 3.1. *Let q be a prime power, $n \geq q$, $m \geq n^{3\log_2 n}$, and $\Gamma \subseteq \mathbf{F}_{q^n}$ with $\#\Gamma \leq n$. Consider arithmetic circuits with free qth powers, constants from Γ, and which are defined for at least m nonzero elements of $\mathbf{F}_{q^n}$. Then there exists $e \in \mathbf{N}$ with $0 \leq e < q^n$ such that any such circuit value-computing π_F^e has size at least*

$$\frac{\log_2 m}{3\log_2 n} \cdot \left(1 - \frac{2}{\log_2 n}\right).$$

PROOF. Let $\gamma = \#\Gamma$, and $\Gamma = \{c_1, \ldots, c_\gamma\}$. Let α be an arithmetic circuit over $F = \mathbf{F}_{q^n}$ of size ℓ using constants from Γ, and free qth powers. As above, we use $f_v \in F(x)$ for a gate v. We number the gates of α as

$$v_{-\gamma}, \ldots, v_{-1}, v_0, v_1, \ldots, v_\ell,$$

with constant gates $v_{-\gamma}, \ldots, v_{-1}$ (and $f_{v_{-i}} = c_i$ for $i \geq 1$), $f_{v_0} = x$, and such that for each i with $1 \leq i \leq \ell$ there exist $j, k, e_1, e_2 \in \mathbf{Z}$ and $\circ \in \{+, -, *, /\}$ such that

$$f_{v_i} = (f_{v_j})^{q^{e_1}} \circ (f_{v_k})^{q^{e_2}}, \quad -\gamma \leq j, k < i, \ e_1, e_2 \in \mathbf{N}. \tag{3.2}$$

It is clear that each circuit of size at most ℓ can be brought into this form. Since $a^{q^n} = a$ for all $a \in F$ and we only consider "value-computing", we may assume that $0 \leq e_1, e_2 < n$ in (3.2). We can normalize the circuit so that $e_1 = 0$ in (3.2), replacing f_{v_i} by

$$f_{v_i}^{q^{n-e_1}} = f_{v_j} \circ f_{v_k}^{q^{e_2+n-e_1}},$$

and reducing the exponent $e_2 + n - e_1$ modulo n, inductively for $i = 1, \ldots, \ell$. At gate v_i with $i \geq 1$, there are $(\gamma+i)^2 \cdot n \cdot 4$ possible choices for the parameters $j, k, e_2, \circ$, and hence there are at most

$$\prod_{1 \leq i \leq \ell} 4n(\gamma + i)^2 \leq (4n)^\ell (\gamma + \ell)^{2\ell}$$

such circuits. Let α be such a circuit, $f = f_{v_\ell} \in F(x)$ the function computed, $A \subseteq F$ the set of nonzero elements at which α is defined, and suppose that α value-computes π_F^e for some e with $0 \le e < q^n$. Then $\#A \ge m$, and there exists $d \in \mathbf{N}$ such that $0 \le d < n$, $f(a)$ is defined and $f(a)^{q^d} = a^e$ for all $a \in A$. By Lemma 3.2 below, for each i with $0 \le i < q^n/m$ there is at most one such e with $im \le e < (i+1)m$ (i.e., e is uniquely determined by f, d, i), and hence α value-computes π_F^e for at most $n \cdot \lceil q^n/m \rceil$ many e's.

We have the following inequalities:

$$
\begin{aligned}
6(\log_2 n)^3 &\le 2\log_2 n \cdot \log_2 m < 2\log_2 n \cdot \log_2 m + 8\log_2 m\,, \\
&\log_2 m \cdot (\log_2 n - 2) \cdot (3\log_2 n + 4) \\
&< (\log_2 m - 2\log_2 n) \cdot 3(\log_2 n)^2 \qquad (3.3) \\
&\le (\log_2 m - \log_2 n - 1) \cdot 3\log_2 n \cdot \log_2 n\,.
\end{aligned}
$$

Now suppose that all powers π_F^e with $0 \le e < q^n$ can be value-computed with size ℓ. We may assume that $\ell \le n$. By the above we have

$$
q^n \le n\lceil q^n/m \rceil \cdot (4n)^\ell (\gamma + \ell)^{2\ell} \le n(q^n + m)/m \cdot (16n^3)^\ell, \qquad (3.4)
$$

$$
\ell \ge \frac{\log_2 \frac{mq^n}{n(q^n+m)}}{3\log_2 n + 4} > \frac{\log_2 m - \log_2 n - 1}{3\log_2 n + 4} \ge \frac{\log_2 m}{3\log_q n} \cdot \left(1 - \frac{2}{\log_2 n}\right). \qquad (3.5)
$$

The second inequality in (3.5) follows from $m < q^n$, and the last one from (3.3). □

LEMMA 3.2. *Let $g, h \in \mathsf{F}_{q^n}[x]$ with $\gcd(g,h) = 1$, $j \in \mathbf{N}$, and $A \subseteq \mathsf{F}_{q^n} \setminus \{0\}$. Then there is at most one $e \in \mathbf{N}$ with $h(a) \ne 0$ and $g(a)/h(a) = a^e$ for all $a \in A$ and $j \le e < j + \#A$.*

PROOF. Suppose that $(g - x^e h)(a) = 0$ for all $a \in A$, and let

$$
u = \prod_{a \in A} (x - a) \in \mathsf{F}_{q^n}[x].
$$

Then u divides $g - x^e h$. Let v be the (monic) gcd of h and u in $\mathsf{F}_{q^n}[x]$. Then $v \mid g$, hence $v = 1$ and h is invertible modulo u. It follows that $x^e \equiv g/h \bmod u$. There is exactly one polynomial of degree less than $\#A = \deg u$ satisfying this congruence; this proves the claim for $j = 0$ (and we do not use that $0 \notin A$).

Suppose that $e < j + \#A$, and that $(g - x^d h)(a) = 0$ for all $a \in A$ and some d with $j \le d \le e$. Then

$$
u \mid (g - x^d h) - (g - x^e h) = x^d h \cdot \left(x^{e-d} - 1\right),
$$

and hence $u \mid x^{e-d} - 1$. But since $e - d < \deg u$, we have $x^{e-d} - 1 = 0$ and $e = d$. □

As is usual in counting arguments, the lower bound hold for "most e". In fact, given $\epsilon > 0$, it is easy to work out a lower bound that holds for all e with at most $\epsilon \cdot q^n$ exceptions.

In Theorem 3.1, it is unavoidable to assume that the circuits are defined at sufficiently many elements, since $1/(x^{q^n} - x)$ can be computed in size 2, and the corresponding circuit is defined nowhere and trivially value-computes $\pi^e_{\mathbf{F}_{q^n}}$ for any e.

COROLLARY 3.3. *Let q be a prime power, $n \geq q$, and $\Gamma \subseteq \mathbf{F}_{q^n}$ with $\#\Gamma \leq n$.*

(i) If $n \geq q^5$ and either $q \geq 3$ or $n \geq 626$, then any x^e with $0 \leq e < q^n$ can be computed in size

$$\frac{n}{\log_q n}\left(1 + \frac{10 \log_q \log_q n + 6}{\log_q n}\right).$$

(ii) Let $\Omega = \{+, -, *\}$ or $\Omega = \{*, /\}$, and consider arithmetic circuits with operations from Ω, free qth powers, and only constants from Γ. Then there exists $e \in \mathbf{N}$ with $0 \leq e < q^n$ such that any such circuit value-computing π^e_F has size at least

$$\frac{n}{3 \log_q n} \cdot \left(1 - \frac{2}{\log_2 n}\right).$$

PROOF. The upper bound comes from Corollary 2.3 (i). For the lower bound we note that, in the notation of the proof of Theorem 3.1, $A = \mathbf{F}_{q^n} \setminus \{0\}$ and any (α, d) determine e uniquely except that for $\Omega = \{*, /\}$, $e = 0$ and $e = q^n - 1$ can both happen. Since we can assume $0 \leq d < n$, there are at most n values e such that α value-computes π^e_F. (In the exceptional case, there are exactly two such e, since then $f(a)^q = f(a) = 1$ for nonzero a.) Furthermore, we can replace the four choices for $\circ$ by at most three, and thus (3.4) becomes

$$q^n \leq n \cdot (3n)^\ell \cdot (\gamma + \ell)^{2\ell} \leq n \left(12n^3\right)^\ell.$$

A calculation yields the bound. □

Under the hypotheses of Corollary 3.3 (ii), we obtain from (2.1) width at least $n/(3c \log_2^2 n) \cdot (1 - 2/\log_q n)$ if the depth is at most $c \log_2 n$.

The upper and lower bounds have a gap of a factor of 3. To close this gap, we observe that Algorithm 2 can be arranged so that for all $i > \beta\ell$, (3.2) has the special form $f_i = f_{i-1} * f_j^{q^{i-k}}$ for some j, $0 \le j < i$, with β about $(\log_q n)^{-1}$ and a fixed $k \le \beta\ell$. For such artificially contrived circuits, the counting argument yields indeed $\ell \ge (n/\log_q n)(1 - O((\log_q n)^{-1}))$ for some e.

If we consider general arithmetic circuits, with $+, -, *, /$, at most q constants, and free qth powers, and the stronger notion of computing x^e, then the counting argument will again show that the size is at least $n/(3\log_q n)\cdot(1-o(1))$ for some e.

The following questions remain open.

- Describe a specific e so that $\pi^e_{\mathbf{F}_{q^n}}$ requires size $\Omega(n/\log_q n)$.
- Either improve the width to $o(n/\log_q n)$, or prove that the width is $\Omega(n/\log_q n)$, assuming depth $O(\log n)$.
- Prove that the size is not less than $n/\log_q n + o(n/\log_q n)$ for some e.

4. Addition/subtraction chains with free multiples

The purpose of the remainder of this paper is to study the *parallel complexity* of the exponentiation problem, with free qth powers. Only Theorem 4.1 and Proposition 4.4 deal with general arithmetic circuits. Otherwise we consider abstractions of algorithms using only multiplication, or only multiplication and divisions, namely *addition chains* and *addition/subtraction chains*. We determine the parallel complexity of exponentiation *exactly* in this model.

Compared to the results of Section 3, the bounds of this section have the special appeal of being sharp and for individual e, and the drawback that they refer to exact computation of x^e (respectively e); this is partly addressed in Theorem 7.3.

In the usual model of arithmetic circuits (without free qth powers) this parallel complexity has been investigated: upper bounds $O(\log^2 n)$ are in Golovanov & Solodovnikov (1987) and Fich & Tompa (1988), $O(\log n)$ in von zur Gathen (1990), all for circuits over $\mathbf{F}_q$, and lower bounds $\Omega(n \log q)$ for circuits over $\mathbf{F}_{q^n}$ in von zur Gathen (1987) and von zur Gathen & Seroussi (1991).

For $e \in \mathbf{N}$ with q-ary representation $e = \sum_{i \geq 0} e_i q^i$, let

$$\sigma_q(e) = \sum_{i \geq 0} e_i$$

be the sum of digits. Thus $\sigma_q(0) = 0$. Note that for $d, e, j \in \mathbf{N}$ we have $\sigma_q(e) \leq (q-1)\lceil \log_q e \rceil$, and

$$\sigma_q(q^j d) = \sigma_q(d), \quad \sigma_q(d+e) \leq \sigma_q(d) + \sigma_q(e), \tag{4.1}$$

with equality in the subadditivity if and only if $d_i + e_i < q$ for all i.

(4.1) implies that σ_q(exponent) can at most double in one multiplication (with free qth powers), and if x^e is computed in depth δ, we have

$$\delta \geq \lceil \log_2 \sigma_q(e) \rceil .$$

This holds for circuits with addition as well:

THEOREM 4.1. *Let $1 \leq e < q^n$. The depth of any arithmetic circuit over $\mathbf{F}_{q^n}$ computing x^e using $+, -, *$, and free qth powers, is at least $\lceil \log_2 \sigma_q(e) \rceil$.*

PROOF. Suppose α is an arithmetic circuit as above computing x^e. For any

$$f = f_{i_1} x^{i_1} + \cdots + f_{i_t} x^{i_t} \in \mathbf{F}_{q^n}[x] \tag{4.2}$$

with $i_1, \ldots, i_t \in \mathbf{N}$ pairwise distinct and $f_{i_1}, \ldots, f_{i_t} \in \mathbf{F}_{q^n}$, let

$$\sigma_q(f) = \max\{\sigma_q(i_1), \ldots, \sigma_q(i_t)\} .$$

(Thus $\sigma_2(x^7 + x^2) = 3$.) For any gate v of α, let $f_v \in \mathbf{F}_{q^n}[x]$ be the function computed at v. At an addition or subtraction gate (3.1) with $\circ \in \{+, -\}$ we have $\sigma_q(f_v) \leq \max\{\sigma_q(f_{w_1}), \sigma_q(f_{w_2})\}$. At a multiplication gate, we have $\sigma_q(f_v) \leq \sigma_q(f_{w_1}) + \sigma_q(f_{w_2})$. By induction on the depth, it follows that for a gate v at depth i we have $\sigma_q(f_v) \leq 2^i$. Hence $\log_2 \sigma_q(e) = \log_2 \sigma_q(f_{v_\ell}) \leq \mathrm{depth}(\alpha)$, where v_ℓ is the output gate. □

A very simple type of arithmetic circuit consists just of multiplications and qth powers, as in Section 2. Thus only powers x^d are computed, for various $d \in \mathbf{N}$. This type of circuit corresponds to *addition chains*, where each step is an addition of two previous integers, starting with the constant 1. An excellent survey of addition chains is in Knuth (1982, 4.6.3). Free qth powers in the circuit correspond to *free multiplications by q* in the addition chain. These chains, and a slight generalization, will be our model for the remainder of the

paper. In particular, q is now an arbitrary integer at least two (except in Proposition 4.4).

We first show how the lower bound of Theorem 4.1 can be achieved. We expand each q-ary digit of e in unary and compute e by a binary tree of additions, with free multiplications by q, using these unary digits as leaves and ignoring q-ary digits which are zero.

EXAMPLE 4.2. *Take $q = 8$ and $e = 60423$, with octal representation $(166007)_8$ and $\sigma_8(e) = 20$. Then the following gives an addition chain of depth 5 and size 19 (all numbers are in decimal):*

$$\underbrace{\underbrace{\underbrace{\underbrace{1}_{1}\,\underbrace{1}_{1}}_{2}\,\underbrace{\underbrace{1}_{1}\,\underbrace{1}_{1}}_{2}}_{4}\,\underbrace{\underbrace{\underbrace{1}_{1}\,\underbrace{1}_{1}}_{2}\,\underbrace{\underbrace{1}_{1}\,\underbrace{1}_{1}}_{2}}_{4}}_{8}\,\underbrace{\underbrace{\underbrace{\underbrace{1}_{1}\,\underbrace{0}_{0}}_{2}\,\underbrace{\underbrace{0}_{0}\,\underbrace{1}_{1}}_{2}}_{4}}_{8}\,\underbrace{\underbrace{1}_{1}\,\underbrace{1}_{1}}_{2}}_{16}\,\underbrace{\underbrace{1}_{1}\,\underbrace{1}_{1}}_{2}}_{32}\,\underbrace{\underbrace{1}_{1}\,\underbrace{1}_{1}}_{2}}_{64}$$

In this example, we have used powers of 8 as late as possible. For a general description, it is easier to use the required powers of q right away, so that the leftmost 9 in the second row above becomes a $9 \cdot 8^4$. In fact, we could arrange the leaves q^i in any order; this will be used in the proof of Theorem 4.5 below. Formally, we build a binary tree of additions whose leaves are indexed by

$$I = \{(i,j) : i \geq 0 \text{ and } 1 \leq j \leq e_i\},$$

and where the value at leaf (i,j) is q^i. This leads, in general, to an addition chain of depth $\lceil \log_2 \sigma_q(e) \rceil$ and size $\sigma_q(e) - 1$. Thus we have the following result.

THEOREM 4.3. *Let $e, q \geq 2$. The minimal depth of addition chains for e with free multiplication by q is exactly $\lceil \log_2 \sigma_q(e) \rceil$. It can be achieved with size $\sigma_q(e) - 1$. The maximum value of $\sigma_q(d)$ for $1 \leq d < q^n$ is $\sigma_q(q^n - 1) = (q-1)n$.*

When we also allow subtractions, the lower bound seems to break down, since the worst case of Theorem 4.3, namely $q^n - 1$, can be computed in one step (with free multiplication by q). However, the lower bound survives in the following form.

An *addition/subtraction chain with free multiplication by q* has constants 1 and -1, and each gate is an addition or subtraction of two previous values,

each multiplied by some power q^i of q, with $i \in \mathbf{N}$. Such a chain *computes* e if $e = q^i d$ for some value d occurring in the chain, and $i \in \mathbf{N}$.

For $e \in \mathbf{Z}$ define

$$\sigma_q^{\pm}(e) = \min\{\sigma_q(a) + \sigma_q(b) : a, b \in \mathbf{N},\ e = a - b\}. \tag{4.3}$$

Similar to (4.1), we have for $e, d \in \mathbf{Z}$ and $i \in \mathbf{N}$

$$\sigma_q^{\pm}(e) = \sigma_q^{\pm}(-e), \quad \sigma_q^{\pm}(q^i e) = \sigma_q^{\pm}(e), \quad \sigma_q^{\pm}(d+e) \leq \sigma_q^{\pm}(d) + \sigma_q^{\pm}(e). \tag{4.4}$$

The second equality follows from the fact that any minimal representation $qd = a - b$ will have $a_0 = b_0 = 0$ (see I in the proof of Theorem 5.4 below). Instead of writing $e = a - b$, it is equivalent to consider "signed-digit representations" $e = \sum_{i \geq 0} e_i q^i$ with digits e_i from $-(q-1)$ to $q-1$. For $q = 2$, arithmetic based on this representation is discussed extensively in Reitwiesner (1960).

We start with a lower bound for general arithmetic circuits with free qth powers.

PROPOSITION 4.4. *Let $1 \leq e < q^n$, and α an arithmetic circuit with free qth powers computing $x^e \in \mathbf{F}_{q^n}[x]$. Then the depth of α is at least $\log_2 \sigma_q^{\pm}(e) - 1$.*

PROOF. For

$$f = f_{i_1} x^{i_1} + \cdots + f_{i_t} x^{i_t} \in F[x]$$

as in (4.2), we let

$$\sigma_q^{\pm}(f) = \max\{\sigma_q^{\pm}(i_1), \ldots, \sigma_q^{\pm}(i_t)\}.$$

Instead of the rational function $f_v \in F(x)$ computed at a gate v, we keep track of an explicit numerator $n_v \in F[x]$ and denominator $d_v \in F[x]$, with $f_v = n_v/d_v$, defined inductively in the natural way, but possibly with common factors. For a constant or input gate v, we have $n_v = f_v$ and $d_v = 1$. At a gate v, with $w_1, w_2, e_1, e_2, \circ$ as in (3.1), we set $(N_i, D_i) = (n_{w_i}^{q^{e_i}}, d_{w_i}^{q^{e_i}})$ for $i = 1, 2$, and then

$$(n_v, d_v) = \begin{cases} (N_1 D_2 \pm D_1 N_2, D_1 D_2) & \text{if } \circ = \pm, \\ (N_1 N_2, D_1 D_2) & \text{if } \circ = *, \\ (N_1 D_2, D_1 N_2) & \text{if } \circ = /, \end{cases}$$

$$s_v = \max\{\sigma_q^{\pm}(n_v), \sigma_q^{\pm}(d_v)\}.$$

Clearly $\sigma_q^{\pm}$ is invariant under qth powers, by (4.4), and one verifies that

$$s_v \leq s_{w_1} + s_{w_2}.$$

By induction on the depth i of v, this implies that $s_v \le 2^i$ for all gates v. Now let v be the output gate, and δ its depth. Then $(n_v/d_v)^{q^d} = x^e$ for some $d \in \mathbf{N}$. It follows that q^d divides e and $n_v/d_v = x^{e'}$ with $e' = eq^{-d}$. Write $d_v = f_{i_1}x^{i_1} + \cdots + f_{i_t}x^{i_t}$, as in (4.2); then $n_v = f_{i_1}x^{i_1+e'} + \cdots + f_{i_t}x^{i_t+e'}$.

Choose some k, $1 \le k \le t$, with

$$s_v = \max\{\sigma_q^{\pm}(n_v), \sigma_q^{\pm}(d_v)\} = \max\{\sigma_q^{\pm}(i_k + e'), \sigma_q^{\pm}(i_k)\}.$$

Then, using (4.4), we have

$$\begin{aligned} \sigma_q^{\pm}(e) = \sigma_q^{\pm}(e') &\le \sigma_q^{\pm}(i_k + e') + \sigma_q^{\pm}(-i_k) \\ &\le 2\max\{\sigma_q^{\pm}(n_v), \sigma_q^{\pm}(d_v)\} = 2s_v \le 2^{\delta+1}. \end{aligned}$$ □

THEOREM 4.5. *Let $e, q \in \mathbf{Z}$, $e \neq 0$, $q \ge 2$. The minimal depth of addition/subtraction chains computing e with free multiplication by q is exactly $\lceil \log_2 \sigma_q^{\pm}(e) \rceil$. It can be achieved with size $\sigma_q^{\pm}(e) - 1$.*

PROOF. For the lower bound, suppose we have an addition/subtraction chain γ computing e. At each gate v of γ some $e_v \in \mathbf{Z}$ is computed, and $q^d e_v = e$ for some gate v and $d \in \mathbf{N}$. Denote by $D(v)$ the depth of v, i.e., the length (= number of $\pm$-gates) of a longest path from the start nodes (with values 1 and -1) to v. We show by induction on $D(v)$ that

$$\sigma_q^{\pm}(e_v) \le 2^{D(v)}.$$

The lower bound then follows, using (4.4). The claim is clear at depth zero, where $e_v = 1$ or $e_v = -1$. So let $D(v) \ge 1$. There exist gates w_1, w_2 of γ and integers $i_1, i_2 \in \mathbf{N}$ so that

$$e_v = q^{i_1}e_{w_1} \pm q^{i_2}e_{w_2},$$

and $D(w_1), D(w_2) < D(v)$. For $j = 1, 2$, choose $a_j, b_j \in \mathbf{N}$ with $e_{w_j} = a_j - b_j$ and $\sigma_q^{\pm}(e_{w_j}) = \sigma_q(a_j) + \sigma_q(b_j)$. Then

$$e_v = \begin{cases} (q^{i_1}a_1 + q^{i_2}a_2) - (q^{i_1}b_1 + q^{i_2}b_2) & \text{if } v \text{ is a } +\text{-gate} \\ (q^{i_1}a_1 + q^{i_2}b_2) - (q^{i_1}b_1 + q^{i_2}a_2) & \text{if } v \text{ is a } -\text{-gate} \end{cases}$$

In the first case, we have

$$\begin{aligned} \sigma_q^{\pm}(e_v) &\le \sigma_q(q^{i_1}a_1 + q^{i_2}a_2) + \sigma_q(q^{i_1}b_1 + q^{i_2}b_2) \\ &\le \sigma_q(a_1) + \sigma_q(a_2) + \sigma_q(b_1) + \sigma_q(b_2) \\ &\le 2^{D(w_1)} + 2^{D(w_2)} \le 2^{D(v)}. \end{aligned}$$

The second case follows analogously.

For the upper bound, let $e = a - b$. We claim that e can be computed in depth $\delta = \lceil \log_2(\sigma_q(a) + \sigma_q(b)) \rceil$; see Example 4.6 for an illustration.

We write a_i and b_i for the q-ary digits of a and b, respectively, and expand each q-ary digit of a and b in unary: $a_{ij} = 1$ for $i \geq 0$ and $1 \leq j \leq a_i$; and similarly for b. Let

$$I = \{(i,j) : i \geq 0 \text{ and } 1 \leq j \leq b_i\}$$

be the nonzero positions in the unary expansion of the q-ary representation of b, so that $\sigma_q(b) = \#I$. There is an asymmetry in that $x \pm y$ can be computed in one step from x and y, but not $-x - y$. Because of this asymmetry, we distinguish two cases.

As a first case, we consider $\sigma_q(a) \geq \sigma_q(b)$. To each $(i,j) \in I$ we associate the index (u_{ij}, v_{ij}) of a unary digit of a, with $v_{ij} \leq a_{u_{ij}}$, so that these (u_{ij}, v_{ij}) are all distinct. Using the construction for Theorem 4.3, we can find an addition chain for $a + b$ of depth δ, where at depth 1 all $q^{u_{ij}} + q^i$ are computed, for $(i,j) \in I$. Replacing each such addition by $q^{u_{ij}} - q^i$, the resulting addition/subtraction chain computes e, still in depth δ.

For the case $\sigma_q(b) > \sigma_q(a)$, we proceed by induction on δ. In the case $\delta = 0$ (so that $\sigma_q(b) = 1$, $a = 0$), the claim is clear. So let $\delta \geq 1$, and choose a subset $I' \subseteq I$ with

$$\#I' = \min\{2^{\delta-1}, \#I\}.$$

Now $b' = \sum_{(i,j) \in I'} q^i$ can be computed by an addition chain of depth $\delta - 1$, by Theorem 4.3. We let $a' = a - \sum_{(i,j) \in I \setminus I'} q^i$, and note that $a' \neq 0$ and

$$\sigma_q(a) + \#(I \setminus I') \leq 2^{\delta-1}.$$

Thus a' can be computed by an addition/subtraction chain of depth at most $\delta - 1$, using the first case if $\sigma_q(a) \geq \#(I \setminus I')$, and the induction hypothesis otherwise. Finally, $e = a' - b'$ is computed in depth δ.

In each case, it is easy to verify the claim about the size. □

EXAMPLE 4.6. *We consider* $q = 8, n = 6$, $e = 60423$ *with octal representation* $(166007)_8$ *as in Example 4.2, with* $\sigma_8(e) = 20$ *and* $\sigma_8^{\pm}(e) = 7$, *given by the following octal addition, according to Theorem 5.4:*

$$\begin{array}{rr} e: & 166007 \\ b: & 012001 \\ \hline a: & 200010 \end{array}$$

Then we have the following addition/subtraction chain for e, of depth 3 and size 6:

$$\begin{array}{cccccccc} 0 & & -1 & -1 & -1 & 0 & 0 & -1 \\ 1 & 1 & 0 & & 0 & 0 & 1 & 0 \end{array}$$

$$\underbrace{\underbrace{\underbrace{2}_{}\quad\underbrace{-9}_{}}_{119}\quad\underbrace{\underbrace{-63}_{}}_{-505}}_{60423}$$

The maximum value $\lfloor n(q-1)/2 \rfloor + 1$ of $\sigma_q^{\pm}(e)$ for $0 \leq e < q^n$ will be derived in Section 6.

Note that if $e \leq -1$, then $\sigma_q^{\pm}(e) = \sigma_q^{\pm}(-e)$, and an addition/subtraction chain for $-e$ becomes one for e by simply interchanging the roles of the constant gates 1 and -1. If we disallow the constant -1 in addition/subtraction chains, using only the constant 1, then the depth may increase (e.g., from 0 to 2 for $e = -q^i$). However, at depth two we then have also $e = -1$ available, and thus the depth never increases by more than two.

The proof of Theorem 4.5 shows that allowing to compute $-e_1 - e_2$ in one step from e_1 and e_2 does not decrease the minimal depth.

If $1, \ldots, q-1$ are given for free, one finds $\lceil \log_2 w_q(e) \rceil$ and $\lceil \log_2 w_q^{\pm}(e) \rceil$ for the minimal depth of addition chains and addition/subtraction chains, respectively, where $w_q(e)$ is the q-ary weight of e as in (2.2), and $w_q^{\pm}$ is defined in analogy with (4.3).

For practical purposes, it may be advantageous to compute -1 first (i.e., a^{-1} for the exponentiation problem) and then only perform additions. This increases the size and depth by at most one.

5. Constructing an addition/subtraction chain of optimal depth

Now that we have determined the parallel complexity in our addition/subtraction chain model, we want to efficiently exhibit an optimal algorithm. This actually turns out to be somewhat trickier than finding the complexity.

Reitwiesner (1960) solves this problem for $q = 2$, and in fact shows that there is a unique "minimal" representation $e = a - b$ in which two adjacent positions never have both a nonzero entry (i.e., $(a_i + b_i)(a_{i+1} + b_{i+1}) = 0$ for

all i), that this representation provides minimal $\sigma_2^{\pm}(e)$, and gives an algorithm to compute this (a, b). Jedwab & Mitchell (1989) suggest the use of divisions in modular exponentiation, and exhibit an algorithm that finds the above minimal (a, b) and $\sigma_2^{\pm}(e)$, and also an optimal addition/subtraction chain for $q = 2$.

By Theorem 4.5, given $e \in \mathbf{N}$ it is sufficient to find $a, b \in \mathbf{N}$ with $e = a - b$ and minimal $\sigma_q(a) + \sigma_q(b)$. As usual, we have an integer $q \geq 2$, $0 \leq e < q^n$, and let $(e_{n-1}, e_{n-2}, \ldots, e_1, e_0)$ be the q-ary representation of e, with $e = \sum e_i q^i$ and $e_{n-1}, \ldots, e_0 \in \{0, \ldots, q-1\}$. We also set $e_n = e_{-1} = 0$. Let $m = (q-1)/2$. We define a *block* for e as an interval of indices $B = \{j, j-1, \ldots, k+1, k\}$ with $n > j \geq k \geq 0$, $e_j, \ldots, e_k \geq m > e_{j+1}$, $e_k > m \geq e_{k-1}$, and either $j > k$ or $e_k > q/2$. Furthermore, $e_i < m$ for the largest i with $k > i \geq -1$ and $e_i \neq m$. The *right endpoint* of this block is k. Let

$$\mathcal{B} = \{i : i \in B \text{ for some block } B\} \tag{5.1}$$

be the set of all indices occurring in some block.

The definitions of this paragraph are relevant only for even q. An index i is a *bump* if $i \notin \mathcal{B}$ and $e_i = q/2$. A *bridge* is an interval $D = \{j, \ldots, k\}$ consisting of alternating values $(q-2)/2, q/2, (q-2)/2, q/2, \ldots, q/2, (q-2)/2$ beginning and ending with $(q-2)/2$, and with $j+1,\ k-1 \in \mathcal{B}$ and $j \geq k$. We let

$$\mathcal{D} = \{i : i \in D \text{ for some bridge } D\} \tag{5.2}$$

be the set of all indices occurring in some bridge.

Furthermore, we define

$$\begin{aligned} \beta &= \beta(e) = \text{number of blocks}, \\ \gamma &= \gamma(e) = \text{number of bumps}, \\ \delta &= \delta(e) = \text{number of bridges}. \end{aligned} \tag{5.3}$$

Thus $\gamma = \delta = 0$ for odd q. For a digit $d \in \{0, \ldots, q-1\}$, we let

$$d^* = \begin{cases} d & \text{if } 0 \leq d \leq (q-1)/2, \\ q-1-d & \text{if } (q-1)/2 < d < q, \end{cases}$$

and finally

$$\tau = \tau(e) = \sum_{0 \leq i < n} e_i^*. \tag{5.4}$$

We now construct a and b achieving the minimum in (4.3), by defining the digits a_i and b_i of a and b, respectively, for $n \geq i \geq 0$. We first set

$$(a_i, b_i) = \begin{cases} (e_i, 0) & \text{if } i \notin \mathcal{B} \cup \mathcal{D}, \\ (0, q-1-e_i) & \text{if } i \in \mathcal{B} \cup \mathcal{D}, \end{cases} \tag{5.5}$$

THEOREM 5.4. *Let $q \geq 2$, $n \in \mathbf{N}$, and $0 \leq e < q^n$. For $a, b \in \mathbf{N}$ with the q-ary digits as constructed above, we have*

(i) $e = a - b$,

(ii) $\sigma_q^{\pm}(e) = \sigma_q(a) + \sigma_q(b)$,

(iii) $\sigma_q^{\pm}(e) = \tau(e) + 2\beta(e) + \gamma(e) - \delta(e)$.

PROOF. (i) Let $c_n, c_{n-1}, \ldots, c_0, c_{-1} \in \{0,1\}$ be the carries produced in the q-ary addition $e + b$, with $c_n = c_{-1} = 0$. We claim that for all i with $0 \leq i < n$ we have

$$c_i = \begin{cases} 1 & \text{if } i \in \mathcal{B} \cup \mathcal{D}, \\ 0 & \text{otherwise,} \end{cases} \tag{5.6}$$

and $e_i + b_i + c_{i-1} = c_i q + a_i$. This will prove that $e = a - b$. The claims are shown by induction on i. For $i = 0$ the addition is:

$$\begin{array}{ll} e: & \cdots \quad e_0 \\ b: & \cdots \quad 0 \\ \hline a: & \cdots \quad e_0 \end{array} \text{ if } 0 \notin \mathcal{B}, \quad \text{and} \quad \begin{array}{ll} e: & \cdots \quad e_0 \\ b: & \cdots \quad q - e_0 \\ \hline a: & \cdots \quad 0 \end{array} \text{ if } 0 \in \mathcal{B}.$$

This proves both claims. For $i > 0$ we distinguish cases according to the construction.

1) If $i \in \mathcal{B}$ is a right endpoint of a block, and $i - 1 \notin \mathcal{D}$, then $c_{i-1} = 0$, $c_i = 1$, and

$$e_i + b_i + c_{i-1} = e_i + (q - e_i) + 0 = q = c_i q + a_i.$$

2) If $i \in \mathcal{B} \cup \mathcal{D}$, but not as in 1), then $c_i = c_{i-1} = 1$, and

$$e_i + b_i + c_{i-1} = e_i + (q - e_i - 1) + 1 = q = c_i q + a_i.$$

3) If $i \notin \mathcal{B} \cup \mathcal{D}$ and $i - 1 \in \mathcal{B}$, then $c_i = 0$, $c_{i-1} = 1$, and

$$e_i + b_i + c_{i-1} = e_i + 0 + 1 = c_i q + a_i.$$

4) If $i \notin \mathcal{B} \cup \mathcal{D}$ and $i - 1 \notin \mathcal{B}$, then $c_i = c_{i-1} = 0$, and

$$e_i + b_i + c_{i-1} = e_i + 0 + 0 = c_i q + a_i.$$

(ii) Now let $u, v \in \mathbb{N}$ with $e = u - v$ and $\sigma_q(u) + \sigma_q(v)$ minimal. We will perform "local transformations" on the digits of u and v which do not increase the sum of digits, and so that the final transformed pair of numbers equals (a, b).

Denote by u_i and v_i the q-ary digits of u and v, respectively, and by $w_i \in \{0, 1\}$ the carry in the ith position of the addition "$e + v$":

$$e_i + v_i + w_{i-1} = w_i q + u_i.$$

We first note the following.

I. If $w_i = 0$, then $u_i = e_i + w_{i-1} < q$ and $v_i = 0$. If $w_i = 1$, then $u_i = 0$ and $v_i = q - (e_i + w_{i-1})$.

Namely, if both u_i and v_i were nonzero, we could subtract 1 from both of them and thus diminish $\sigma_q(u) + \sigma_q(v)$.

By I, u and v are determined by e and $w_n, \ldots, w_0$. We now describe nine properties II—X of u, v, and the w_i's which hold after possibly applying some local transformations. Together they imply that $w_i = c_i$ for all i, and hence that $(u, v) = (a, b)$.

II. If $e_i + w_{i-1} \leq (q-1)/2$, then $w_i = 0$.

To achieve this, suppose that $e_i + w_{i-1} \leq (q-1)/2$, and let $j > i$ be such that $v_k = q - 1$ for $j > k > i$ and $v_j \neq q - 1$. If $w_i = 1$, then using I the addition has the form:

$$\begin{array}{lccccccc} e: & \cdots & e_j & e_{j-1} & \cdots & e_{i+1} & e_i & \cdots \\ v: & \cdots & v_j & q-1 & \cdots & q-1 & q-e_i-w_{i-1} & \cdots \\ \hline u: & \cdots & u_j & 0 & \cdots & 0 & 0 & \cdots \end{array}.$$

This implies that $e_{j-1} = \cdots = e_{i+1} = 0$. We transform u and v to

$$\begin{array}{lccccccc} e: & \cdots & e_j & 0 & \cdots & 0 & e_i & \cdots \\ v': & \cdots & v_j+1 & 0 & \cdots & 0 & 0 & \cdots \\ \hline u': & \cdots & u_j & 0 & \cdots & 0 & e_i + w_{i-1} & \cdots \end{array}.$$

(The digit sequence '626' in Example 5.1 illustrates the first case, and '5530' the second case.) Then $e = u' - v'$, and

$$\begin{aligned} &\sigma_q(u) + \sigma_q(v) - (\sigma_q(u') + \sigma_q(v')) \\ &= (j - i - 1)(q - 1) + q - e_i - w_{i-1} - (1 + e_i + w_{i-1}) \\ &\geq q - 2e_i - 2w_{i-1} - 1 \geq 0. \end{aligned}$$

Thus the transformation of (u, v) to (u', v') does not increase the sum of digits. (In fact, the minimality of u, v implies that if $w_i = 1$ before the transformation, then $j = i + 1$, $u_j = 0$, and $q = 2e_i + 2w_{i-1} + 1$. We had to consider separately the case $v_{i+1} = q - 1$, because $v_{i+1} + 1$ would not be a digit, and then found this to be impossible. A similar non-existent difficulty occurs in IV, VII, and IX below.)

III. If $e_i + w_{i-1} \geq (q+1)/2$, then $w_i = 1$.

To achieve this, suppose that $e_i + w_{i-1} \geq (q+1)/2$, and let $j > i$ be such that $u_k = q - 1$ for $j > k > i$ and $u_j \neq q - 1$. If $w_i = 0$, then using I the addition has the form:

$$\begin{array}{lccccccc} e: & \cdots & e_j & e_{j-1} & \cdots & e_{i+1} & e_i & \cdots \\ v: & \cdots & v_j & 0 & \cdots & 0 & 0 & \cdots \\ \hline u: & \cdots & u_j & q-1 & \cdots & q-1 & e_i + w_{i-1} & \cdots \end{array},$$

and $e_i + w_{i-1} < q$. This implies that $e_{j-1} = \cdots = e_{i+1} = q - 1$. We transform u and v to

$$\begin{array}{lccccccc} e: & \cdots & e_j & q-1 & \cdots & q-1 & e_i & \cdots \\ v': & \cdots & v_j & 0 & \cdots & 0 & q - e_i - w_{i-1} & \cdots \\ \hline u': & \cdots & u_j + 1 & 0 & \cdots & 0 & 0 & \cdots \end{array}.$$

(The digit sequence '04' in Example 5.1 illustrates the first case, and '036' the second case.) Then $e = u' - v'$, and

$$\begin{aligned} &\sigma_q(u) + \sigma_q(v) - (\sigma_q(u') + \sigma_q(v')) \\ &= (j - i - 1)(q - 1) + e_i + w_{i-1} - (1 + q - e_i - w_{i-1}) \\ &\geq 2e_i + 2w_{i-1} - 1 - q \geq 0. \end{aligned}$$

Thus the transformation of (u, v) to (u', v') does not increase the sum of digits. (In fact, if $w_i = 0$ before the transformation, then $j = i + 1$, $v_j = 0$, and $q = 2e_i + 2w_{i-1} - 1$.)

The proof of (i) implies that II and III also hold for c_i, c_{i-1} instead of w_i, w_{i-1}, and thus $c_i = w_i$ follows inductively for all cases covered by II and III, provided we can also show it for all other cases.

If q is odd, in fact all cases are covered, and (ii) is proven.

So we may now assume that q is even. Only the case $e_i + w_{i-1} = q/2$ remains uncovered; thus either $e_i = q/2$ and $w_{i-1} = 0$, or $e_i = (q-2)/2$ and $w_{i-1} = 1$.

IV. If $e_i = q/2$ and $e_{i+1} \geq q/2$, then $w_i = 1$.

Assume that $w_i = 0$. By III, we have that $w_{i-1} = 0$. The addition has one of the two forms

$$\begin{array}{lccccc} e: & \cdots & e_{i+2} & e_{i+1} & q/2 & \cdots \\ v: & \cdots & v_{i+2} & 0 & 0 & \cdots \\ \hline u: & \cdots & u_{i+2} & e_{i+1} & q/2 & \cdots \end{array} \quad \text{or} \quad \begin{array}{lccccc} & \cdots & e_{i+2} & e_{i+1} & q/2 & \cdots \\ & \cdots & v_{i+2} & q-e_{i+1} & 0 & \cdots \\ \hline & \cdots & u_{i+2} & 0 & q/2 & \cdots \end{array}.$$

We transform this to

$$\begin{array}{lccccc} e: & \cdots & e_{i+2} & e_{i+1} & q/2 & \cdots \\ v': & \cdots & v_{i+2} & q-e_{i+1}-1 & q/2 & \cdots \\ \hline u': & \cdots & u'_{i+2} & 0 & 0 & \cdots \end{array}.$$

with $u'_{i+2} = u_{i+2} + (1 - w_{i+1})$. (The digit sequence '44' in Example 5.2 is an illustration.) This transformation does not increase the sum of digits. (In the second form there is a strict decrease, so that this form can, in fact, not occur.)

If $w_{i+1} = 0$ and $u_{i+2} = q-1$, we have to make the appropriate modification: letting $j \geq i+2$ be the smallest index with $u_j \leq q-2$ and transforming $(u_j, u_{j-1}, \ldots, u_{i+2})$ into $(u_j + 1, 0, \ldots, 0)$; this strictly decreases the sum of digits if $j > i+2$, and thus can, in fact, not occur.

V. If $i \in \mathcal{B}$, then $w_i = 1$.

Using I, we may assume $e_i = q/2$ to prove this. By the definition of a block, either $i+1 \in \mathcal{B}$ or $i-1 \in \mathcal{B}$. If $i+1 \in \mathcal{B}$, the claim follows from IV. If $i-1 \in \mathcal{B}$, then either $e_{i-1} \geq (q+2)/2$ or $e_{i-1} = q/2$ (and then $w_{i-1} = 1$ by IV). In both cases, $w_{i-1} = 1$, and hence $w_i = 1$ by III.

VI. If $i \in \mathcal{D}$, then $w_i = 1$.

Suppose $\{j, \ldots, k\}$ is a bridge with $j \geq i \geq k$; thus $e_j = e_k = (q-2)/2$ and $j+1, k-1 \in \mathcal{B}$. By V, we have $w_{j+1} = w_{k-1} = 1$. If there is some i with $j \geq i \geq k$ and $w_i = 0$, then choose a smallest such i. Then $w_{i-1} = 1$, and III implies that $e_i = (q-2)/2$. The addition has the form

$$\begin{array}{lccccc} e: & \cdots & e_{i+2} & e_{i+1} & (q-2)/2 & \cdots \\ v: & \cdots & v_{i+2} & v_{i+1} & 0 & \cdots \\ \hline u: & \cdots & u_{i+2} & u_{i+1} & q/2 & \cdots \end{array}.$$

We transform this to

$$\begin{array}{lccccc} e: & \cdots & e_{i+2} & e_{i+1} & (q-2)/2 & \cdots \\ v': & \cdots & v'_{i+2} & q-e_{i+1}-1 & q/2 & \cdots \\ \hline u': & \cdots & u'_{i+2} & 0 & 0 & \cdots \end{array}.$$

If $w_{i+1} = 1$, then $v_{i+1} = q - e_{i+1}$, and we use $u'_{i+2} = u_{i+2}$ and $v'_{i+2} = v_{i+2}$. The sum of digits decreases by one, and thus this case is impossible. If $w_{i+1} = 0$, then $i+1 \notin \mathcal{B}$ by V, and we have $e_{i+1} = q/2$ and $e_{i+2} = (q-2)/2$. Thus $u_{i+2} \leq (q-2)/2 \leq q-2$, and we can use $u'_{i+2} = u_{i+2} + 1$ and $v'_{i+2} = v_{i+2}$. One checks that the transformation does not increase the sum of digits. (By considering a maximal interval of "$w_i = 0$", one can show that this case can, in fact, not occur.)

VII. If $e_i = (q-2)/2$, and either $e_{i-1} \leq (q-2)/2$ or $e_{i+1} \leq (q-2)/2$, then $i \notin \mathcal{B} \cup \mathcal{D}$ and $w_i = 0$.

We have $i \notin \mathcal{B}$. If $i \in \mathcal{D}$, then we have $e_{i+1}, e_{i-1} \geq q/2$, which is not the case; hence $i \notin \mathcal{D}$. Now assume that $w_i = 1$. Then $w_{i-1} = 1$, by II. We first consider the case $e_{i-1} \leq (q-2)/2$. Then $e_{i-1} = (q-2)/2$ and $w_{i-2} = 1$, by II. Thus the addition has the following form:

$$\begin{array}{lccccc} e: & \cdots & e_{i+1} & (q-2)/2 & (q-2)/2 & \cdots \\ v: & \cdots & v_{i+1} & q/2 & q/2 & \cdots \\ \hline u: & \cdots & u_{i+1} & 0 & 0 & \cdots \end{array}.$$

We transform this to

$$\begin{array}{lccccc} e: & \cdots & e_{i+1} & (q-2)/2 & (q-2)/2 & \cdots \\ v': & \cdots & v_{i+1}+1 & 0 & 0 & \cdots \\ \hline u': & \cdots & u_{i+1} & (q-2)/2 & q/2 & \cdots \end{array}.$$

(The digit sequence '6336' in Example 5.2 is an illustration.) Then $e = u' - v'$, $\sigma_q(u) + \sigma_q(v) = \sigma_q(u') + \sigma_q(v')$, and VII holds. (If $v_{i+1} = q-1$, we have to use the smallest $j > i$ with $e_j \neq q-1$, as in II, only to find that this was impossible anyway.)

The second case is where $e_{i-1} > (q-2)/2$, so that $e_{i+1} \leq (q-2)/2$. Since the case of two consecutive $(q-2)/2$'s has been dealt with, we may assume $e_{i+1} < (q-2)/2$. Then $w_{i+1} = 0$ by II, and the addition has the form

$$\begin{array}{lccccc} e: & \cdots & e_{i+1} & (q-2)/2 & \cdots \\ v: & \cdots & v_{i+1} & q/2 & \cdots \\ \hline u: & \cdots & u_{i+1} & 0 & \cdots \end{array}.$$

Since $w_i = 1$ and $w_{i+1} = 0$, we have $u_{i+1} \geq 1$. We transform this into

$$\begin{array}{lcccc} e: & \cdots & e_{i+1} & (q-2)/2 & \cdots \\ v': & \cdots & v_{i+1} & 0 & \cdots \\ \hline u': & \cdots & u_{i+1}-1 & q/2 & \cdots \end{array}.$$

Now we have $\sigma_q(u') + \sigma_q(v') < \sigma_q(u) + \sigma_q(v)$; this shows that the situation cannot occur at all.

VIII. If $e_i = q/2$ and $w_{i+1} = w_{i-1} = 0$, then $w_i = 0$.

Otherwise we would transform

$$\begin{array}{lcccc} e: & \cdots & e_{i+1} & q/2 & \cdots \\ v: & \cdots & 0 & q/2 & \cdots \\ \hline u: & \cdots & e_{i+1}+1 & 0 & \cdots \end{array}$$

to

$$\begin{array}{lcccc} e: & \cdots & e_{i+1} & q/2 & \cdots \\ v': & \cdots & 0 & 0 & \cdots \\ \hline u': & \cdots & e_{i+1} & q/2 & \cdots \end{array}.$$

IX. If $(e_j, \ldots, e_k)$ is an alternating sequence of $(q-2)/2$ and $q/2$ with $j, k \notin \mathcal{B} \cup \mathcal{D}$ and $j \geq k$, then $w_i = 0$ for $j \geq i \geq k$.

We may assume that $(e_j, \ldots, e_k)$ is a maximal such sequence, and by assumption does not form a bridge. We claim that we are in at least one of the following four cases:

a) $e_{k-1} \leq (q-4)/2$,

b) $e_k = e_{k-1} = (q-2)/2$,

c) $e_{j+1} \leq (q-4)/2$,

d) $e_{j+1} = e_j = (q-2)/2$.

To show this claim, assume that all four conditions are false. Then $e_{k-1}, e_{j+1} \geq (q-2)/2$. If $e_{k-1} = (q-2)/2$, then $e_k = (q-2)/2$ since otherwise $(j, \ldots, k)$ would not be maximal; but this would imply b), and hence $e_{k-1} \geq q/2$. Similarly, $e_{j+1} \geq q/2$. But then $e_k = e_j = (q-2)/2$, since otherwise $k \in \mathcal{B}$ or $j \in \mathcal{B}$. Either $j+1 \notin \mathcal{B}$ or $k-1 \notin \mathcal{B}$, since otherwise $(j, \ldots, k)$ is a bridge. If $k-1 \notin \mathcal{B}$, then $k-2 \notin \mathcal{B}$, and $(j, \ldots, k, k-1)$ would be a longer alternating sequence. Similarly, $j+1 \notin \mathcal{B}$ implies that $j+2 \notin \mathcal{B}$ and that $(j+1, j, \ldots, k, k-1)$ is

a longer alternating sequence. In each case, we have a contradiction, and the claim is proven.

We prove $w_i = 0$ for $j \geq i \geq k$, by induction on $i - k$ in cases a) and b), and by induction on $j - i$ in cases c) and d).

In case a), $w_{k-1} = 0$ by II, and in case b), $w_k = w_{k-1} = 0$ by VII. Assume that $w_i = 1$ for some i, $j \geq i \geq k$, and choose the smallest such i. We have $e_i = q/2$ by II, $e_{i+1} \leq (q-2)/2$ since $i \notin \mathcal{B}$, and $w_{i+1} = 1$ by VIII, so that $e_{i+1} = (q-2)/2$, by II. The addition

$$\begin{array}{lccccc} e: & \cdots & e_{i+2} & (q-2)/2 & q/2 & e_{i-1} & \cdots \\ v: & \cdots & v_{i+2} & q/2 & q/2 & 0 & \cdots \\ \hline u: & \cdots & u_{i+2} & 0 & 0 & e_{i-1} & \cdots \end{array}$$

can be transformed to

$$\begin{array}{lccccc} e: & \cdots & e_{i+2} & (q-2)/2 & q/2 & e_{i-1} & \cdots \\ v': & \cdots & v_{i+2}+1 & 0 & 0 & 0 & \cdots \\ \hline u': & \cdots & u_{i+2} & (q-2)/2 & q/2 & e_{i-1} & \cdots \end{array} .$$

(The digit sequence '0436' in Example 5.2 is an illustration.) If $v_{i+2} = q-1$, we find the smallest $\ell \geq i+2$ with $v_\ell \leq q-2$, and transform $(v_\ell, v_{\ell-1}, \ldots, v_{i+2})$ to $(v_\ell + 1, 0, \ldots, 0)$ without changing $(u_\ell, \ldots, u_{i+2})$; this strictly decreases the sum of digits and therefore cannot occur.

So we now assume that a) and b) are false. In case c), $w_{j+1} = 0$ by II, and in case d), $w_{j+1} = w_j = 0$ by VII. Assume $w_i = 1$ for some i, $j \geq i \geq k$, and choose the largest such i.

If $e_i = (q-2)/2$, then $w_{i-1} = 1$ by II, and we transform the addition

$$\begin{array}{lcccc} e: & \cdots & e_{i+1} & (q-2)/2 & \cdots \\ v: & \cdots & 0 & q/2 & \cdots \\ \hline u: & \cdots & e_{i+1}+1 & 0 & \cdots \end{array}$$

to

$$\begin{array}{lcccc} e: & \cdots & e_{i+1} & (q-2)/2 & \cdots \\ v': & \cdots & 0 & 0 & \cdots \\ \hline u': & \cdots & e_{i+1} & q/2 & \cdots \end{array} .$$

This strictly decreases the sum of digits, and thus cannot occur. (If $q = 2$ and $e_{i+1} = 1$, then v, u', v' are as above, but $(u_{i+2}, u_{i+1}) = (1, 0)$; this can indeed occur.)

If $e_i = q/2$, then $e_{i+1} \leq (q-2)/2$ by III. Furthermore, $e_{i-1} = (q-2)/2$, since $e_{i-1} \geq q/2$ implies $i \in \mathcal{B}$, and $e_{i-1} \leq (q-4)/2$ implies $i = k$ and case a), which we ruled out. We transform the addition

$$\begin{array}{lccccc} e: & \cdots & e_{i+1} & q/2 & (q-2)/2 & \cdots \\ v: & \cdots & 0 & q/2-w_{i-1} & v_{i-1} & \cdots \\ \hline u: & \cdots & e_{i+1}+1 & 0 & u_{i-1} & \cdots \end{array}$$

to

$$\begin{array}{lccccc} e: & \cdots & e_{i+1} & q/2 & (q-2)/2 & \cdots \\ v': & \cdots & 0 & 0 & 0 & \cdots \\ \hline u': & \cdots & e_{i+1} & q/2 & (q-2)/2+w_{i-2} & \cdots \end{array}.$$

Let

$$\begin{aligned} \eta &= \sigma_q(u)+\sigma_q(v)-(\sigma_q(u')+\sigma_q(v')) \\ &= e_{i+1}+1+(q/2-w_{i-1})+u_{i-1}+v_{i-1} \\ &\quad -(e_{i+1}+q/2+(q-2)/2+w_{i-2}) \\ &= u_{i-1}+v_{i-1}-q/2+2-w_{i-1}-w_{i-2}. \end{aligned}$$

If $w_{i-1}=0$, then $u_{i-1}=(q-2)/2+w_{i-2}$, $v_{i-1}=0$, and $\eta=1$. If $w_{i-1}=1$, then $u_{i-1}=0$, $v_{i-1}=(q+2)/2-w_{i-2}$, and $\eta=2-2w_{i-2}\geq 0$. In either case, the transformation does not increase the sum of digits.

X. If $i\notin\mathcal{B}\cup\mathcal{D}$, then $w_i=0$.

This follows from II if $e_i\leq(q-4)/2$, from VII if $e_i=(q-2)/2$ and $e_{i-1}\leq(q-2)/2$ or $e_{i+1}\leq(q-2)/2$, from IX if $e_i=(q-2)/2$ and $e_{i-1}\geq q/2$ and $e_{i+1}\geq q/2$, from II and VIII if $e_i=q/2$ and $e_{i-1}\leq(q-4)/2$ and $e_{i+1}\leq(q-4)/2$, and from IX if $e_i=q/2$ and $e_{i-1}=(q-2)/2$ or $e_{i+1}=(q-2)/2$. One checks that this exhausts all possibilities.

Now V, VI, X, and (5.6) imply that $w_i=c_i$ for all i, and hence (ii).

(iii) It is sufficient to show that

$$\sigma_q(a)+\sigma_q(b)=\tau+2\beta+\gamma-\delta.$$

For $0\leq i\leq n$, let

$$\epsilon_i=a_i+b_i-e_i^*\geq 0 \tag{5.7}$$

be the *excess* over the minimal value e_i^*. Thus $\epsilon_i\in\{0,1\}$, and going back to (5.5) and the following paragraph, we find

$$\begin{aligned} \epsilon_i=1 \iff & (i\notin\mathcal{B}\cup\mathcal{D} \text{ and } i-1\in\mathcal{B}) \text{ or } (i\in\mathcal{B} \text{ and } i-1\notin\mathcal{B}\cup\mathcal{D}) \\ & \text{or } (i\in\mathcal{D} \text{ and } e_i=(q-2)/2) \text{ or } (i\notin\mathcal{B}\cup\mathcal{D} \text{ and } e_i=q/2). \end{aligned} \tag{5.8}$$

It is sufficient to show that

$$\sum_{0\le i\le n} \epsilon_i = 2\beta + \gamma - \delta . \tag{5.9}$$

Let $\{j_1,\dots,k_1\}$, $\{j_2,\dots,k_2\}$, $\dots$, $\{j_s,\dots,k_s\}$ be a maximal sequence of blocks with a bridge $D_\ell = \{k_\ell - 1,\dots,j_{\ell+1}+1\}$ between consecutive blocks, so that $s \ge 1$, $D_\ell \subseteq \mathcal{D}$ for $1 \le \ell < s$, and $j_1 + 1, k_s - 1 \notin \mathcal{B} \cup \mathcal{D}$. (In particular, $\{j_1,\dots,k_s\} \subseteq \mathcal{B} \cup \mathcal{D}$ is a maximal subinterval.) For $j_1 + 1 \ge i \ge k_s$, ϵ_i equals 1 if and only if

$$i = j_1 + 1 \text{ or } i = k_s \text{ or } (i \in \mathcal{D} \text{ and } e_i = (q-2)/2),$$

by (5.8). If $\gamma_\ell = (k_\ell - j_{\ell+1} - 2)/2$ is the number of $q/2$'s in bridge D_ℓ (i.e., the number of bumps in D_ℓ), then there are $\gamma_\ell + 1$ many $(q-2)/2$'s in D_ℓ, and

$$\begin{aligned}\sum_{j_1-1\ge i\ge k_s} \epsilon_i &= 2 + \sum_{1\le \ell<s} (\gamma_\ell + 1) \\ &= 2 + \sum_{1\le \ell<s} \gamma_\ell + s - 1 \\ &= \sum_{1\le \ell<s} \gamma_\ell + 2s - (s-1).\end{aligned}$$

Furthermore, for i not in or adjacent to $\mathcal{B} \cup \mathcal{D}$, $\epsilon_i = 1$ only if $e_i = q/2$ and $i \notin \mathcal{B}$. Adding up, (5.9) follows. □

6. The maximal depth

In this section, we determine the range of values assumed by $\sigma_q^{\pm}(e)$ for $0 \le e < q^n$. $\tau(e)$ is often a reasonable estimator for $\sigma_q^{\pm}(e)$, namely

$$\tau(e) \le \sigma_q^{\pm}(e) \le \tau(e) + n + (n \bmod 2) \tag{6.1}$$

holds for any non-negative $e < q^n$, with $n \bmod 2 \in \{0,1\}$. The left inequality follows from Theorem 5.4 (iii) and $\delta \le \beta$, and for the right inequality, we consider the $\beta+\gamma$ sets $\{i, i-1\}$ for i a bump or i the right endpoint of a block. These sets are disjoint and contained in $\{n-1,\dots,0,-1\}$, hence

$$\sigma_q^{\pm}(e) = \tau(e) + 2\beta + \gamma - \delta \le \tau(e) + 2\beta + \gamma \le \tau(e) + n + (n \bmod 2).$$

For $q \geq 3$, the upper bound is achieved at any e whose q-ary representation $(e_{n-1}, \ldots, e_0)$ has $e_{n-i} \geq (q+1)/2$ for odd i, and $e_{n-i} \leq (q-3)/2$ for even i, such as

$$(q-1, 0, q-1, 0, q-1, 0, \ldots),$$

since then each $(n-i)$ is a block for odd i. For $q = 2$, we always have $\tau(e) = 0$.

What is the maximal value of $\sigma_q^{\pm}(e)$? It turns out to be sometimes smaller than what would be obtained from maximizing $\tau(e)$ in the right hand side of (6.1).

EXAMPLE 6.1. *For $q = 8$, we have some examples with $\sigma_8^{\pm}(e) = \lfloor 7n/2 \rfloor + 1$, for $n = 5$ and $n = 6$:*

$$\frac{44343}{34000}, \frac{43434}{00000}, \frac{43435}{00003}, \frac{443434}{340000}, \frac{443344}{340034}, \frac{434344}{000034}.$$
$$\frac{}{100343}, \frac{}{43434}, \frac{}{43440}, \frac{}{1003434}, \frac{}{1003400}, \frac{}{434400}$$

THEOREM 6.2. *Let $q, n \in \mathbf{N}$, $q \geq 2$. Then the maximal value of $\sigma_q^{\pm}(e)$, for $0 \leq e < q^n$, is $\lfloor n(q-1)/2 \rfloor + 1$.*

PROOF. Set $m = \lfloor (q-1)/2 \rfloor$, and let $0 \leq e < q^n$. We first consider the case that q is odd, and let a, b be as constructed in (5.5) and the subsequent two lines. Since $e_k \geq (q+1)/2$ and $e_{j+1} \leq (q-3)/2$ in a block $(j, \ldots, k)$, we have $a_i, b_i \leq m$ for all i with $0 \leq i < n$, and $a_n + b_n \leq 1$. Thus

$$\sigma_q^{\pm}(e) \leq 1 + nm = \lfloor n(q-1)/2 \rfloor + 1.$$

On the other hand, the e with q-ary representation $(m+1, m, m, \ldots, m)$ has

$$\sigma_q^{\pm}(e) = m - 1 + (n-1)m + 2 = nm + 1,$$

by Theorem 5.4 (iii), and thus the upper bound can be achieved.

Now we consider even q. Using the notation ϵ_i from (5.7), we have

$$\sigma_q^{\pm}(e) = \tau(e) + \sum_{0 \leq i \leq n} \epsilon_i = \sum_{0 \leq i \leq n} (e_i^* + \epsilon_i),$$

and $e_i^* \leq m$ for all i. The idea of the upper bound proof is roughly that every index lies in an interval of even length in which the excess is at most $1/2$ per index on average. More precisely, we claim that for each i, $n - 1 \geq i \geq 1$, we have

$$e_i^* + e_{i-1}^* + \epsilon_i + \epsilon_{i-1} \leq 2m + 1,$$

except if

$$i \notin \mathcal{B} \cup \mathcal{D}, e_i = q/2, e_{i-1} = (q-2)/2, i - 2 \in \mathcal{B}. \tag{6.2}$$

To prove the claim, we may assume that $\epsilon_i = \epsilon_{i-1} = 1$, since $e_i^* \leq m$ for all i. Then, using (5.8), we have one of the following cases:

1. $i \in \mathcal{B}, i-1 \notin \mathcal{B} \cup \mathcal{D}, i-2 \in \mathcal{B}$,
2. $i \notin \mathcal{B} \cup \mathcal{D}, i-1 \in \mathcal{B}, i-2 \notin \mathcal{B} \cup \mathcal{D}$,
3. $i \in \mathcal{D}, e_i = (q-2)/2, i-1 \in \mathcal{B}, i-2 \notin \mathcal{B} \cup \mathcal{D}$,
4. $i \notin \mathcal{B} \cup \mathcal{D}, e_i = q/2, i-1 \notin \mathcal{B} \cup \mathcal{D}, i-2 \in \mathcal{B}$.

In case 1, we have $e_{i-1} \leq (q-3)/2$ and $e^*_{i-1} \leq m-1$. In cases 2 and 3, we have $e_{i-1} > q/2$ and again $e^*_{i-1} \leq m-1$. In case 4, we have $e_{i-1} \leq (q-2)/2$, and either (6.2) or $e_{i-1} \leq (q-3)/2$ and $e^*_{i-1} \leq m-1$. Thus the claim is proven.

Now assume (6.2), and define j by $n+1 \geq j > i$,

$$(e_j, \ldots, e_{i-1}) = (e_j, e_{j-1}, q/2, (q-2)/2, q/2, (q-2)/2, \ldots, q/2, (q-2)/2),$$

and $(e_j, e_{j-1}) \neq (q/2, (q-2)/2)$ (using $e_{n+1} = e_n = 0$). We claim that

$$e^*_j + e^*_{j-1} + \epsilon_j + \epsilon_{j-1} \leq 2m. \tag{6.3}$$

To prove (6.3), first suppose that $e_{j-1} = (q-2)/2$. Then $e_j \neq q/2$ and $j \notin \mathcal{B}$ (since otherwise $i \in \mathcal{D}$), hence $e_j \leq (q-2)/2$. Then $\epsilon_j = \epsilon_{j-1} = 0$. Now suppose that $e_{j-1} \neq (q-2)/2$. Then $e_{j-1} \leq (q-4)/2$, since otherwise $j-1 \in \mathcal{B}$ and $i \in \mathcal{D}$. Then $e^*_{j-1} \leq m-1$, $\epsilon_{j-1} = 0$, and

$$e^*_j + e^*_{j-1} + \epsilon_j + \epsilon_{j-1} \leq m + (m-1) + 1 + 0 = 2m.$$

(6.3) implies that

$$\begin{aligned} \sum_{j \geq k \geq i-1} (e^*_k + \epsilon_k) &\leq 2m + (j-i-2)(m + \frac{1}{2}) + 2m + 2 \\ &= (j-i+2)(m+\frac{1}{2}). \end{aligned}$$

Furthermore, if $j = n+1$, as in the third addition of Example 6.1, then $e_j = e_{j-1} = \epsilon_j = \epsilon_{j-1} = 0$, and

$$\sum_{n \geq k \geq i-1} (e^*_k + \epsilon_k) \leq (n+1-i)(m+\frac{1}{2}) + 1.$$

If $j = n$, then $e_j = \epsilon_j = \epsilon_{j-1} = 0$, $e^*_{j-1} \leq m-1$, and

$$\begin{aligned} \sum_{n \geq k \geq i-1} (e^*_k + \epsilon_k) &\leq m - 1 + (n-i)m + \frac{n-i-2}{2} + 2 \\ &= (n+1-i)(m+\frac{1}{2}) - \frac{1}{2}. \end{aligned}$$

Putting things together, we have shown that the set $\{n-1,\ldots,0\}$ of indices can be partitioned into singletons (i) with $e_i^* + \epsilon_i \le m$, and intervals of even length with excess at most $1/2$ per index, except that the leftmost interval may have excess one more (corresponding to $j = n+1$ as above, or $\epsilon_n = 1$ as in the first and fourth addition of Example 6.1). Thus

$$\sigma_q^{\pm}(e) \le n \cdot m + \lfloor n/2 \rfloor + 1 = \lfloor n(q-1)/2 \rfloor + 1.$$

To show that this bound can be achieved, we consider the e with q-ary representation

$$(q/2, q/2, (q-2)/2, q/2, (q-2)/2, q/2, \ldots),$$

as the first and fourth addition in Example 6.1. Then $\tau(e) = nm$, $\beta(e) = 1$, $\gamma(e) = \lfloor (n-2)/2 \rfloor$, $\delta(e) = 0$, so that $\sigma_q^{\pm}(e) = nm + 2 + \lfloor (n-2)/2 \rfloor = \lfloor n(q-1)/2 \rfloor + 1$. □

COROLLARY 6.3. *Let $q \ge 2$, $n \in \mathbb{N}$, $0 \le e < q^n$, and $\ell = \lceil \log_2 n(q-1) \rceil$. Then e can be computed by an addition/subtraction chain with free multiplication by q of depth ℓ, and if $n(q-1)$ is not a power of two, of depth $\ell - 1$.*

For large n and randomly chosen e with $0 \le e < q^n$, the expected value of $\sigma_q^{\pm}(e)$ is approximately $n(q-1)(q+1)/4q$ if q is odd, and $n(q-1)(q+2)/4(q+1)$ if q is even. For large q, this confirms the intuition that $\sigma_q^{\pm}(e)$ should be on average about half as large as the expected value $n(q-1)/2$ of $\sigma_q(e)$.

7. Fermat's Little Theorem

In our usual notation, suppose that $0 \le e < q^n$. What is the relation between arithmetic circuits value-computing $\pi^e_{\mathbf{F}_{q^n}}$ using only multiplication (or multiplication and division) and free qth powers, and addition (or addition/subtraction) chains with free multiplication by q computing e? Obviously, any chain gives an arithmetic circuit computing x^e, without changing size or depth. On the other hand, an arithmetic circuit α as above computing x^e yields a chain for e. But "value-computes", as defined in Section 3, only requires α to compute some x^d with $a^d = a^e$ for all $a \in \mathbf{F}_{q^n}$. If a division occurs in α, this is required

only for $a \neq 0$; in the following, we work with this condition. From Fermat's Little Theorem

$$\forall a \in \mathbf{F}_{q^n} \setminus \{0\} \quad a^{q^n-1} = 1,$$

we find that

$$d \equiv e \bmod q^n - 1$$

is a necessary and sufficient condition. It is somewhat surprising that $d > e$ may actually be advantageous:

EXAMPLE 7.1. *For $q = 8$, $n = 3$, $e = 342$, with octal representation $(526)_8$, and $d = e + 7 \cdot (8^3 - 1) = 3919 = (7517)_8$, we have $\sigma_8^{\pm}(e) = 9 > 7 = \sigma_8^{\pm}(d)$. The two optimal octal additions are:*

$$\begin{array}{rcr} e & = & 526 \\ & & \underline{302} \\ & & 1030 \end{array} \quad , \qquad \begin{array}{rcr} d & = & 7517 \\ & & \underline{301} \\ & & 10020 \end{array} \quad .$$

By Theorem 4.5, x^e requires depth 4, while x^d can be computed in depth 3.

We now prove that if we add $s(q^n - 1)$ to e for small s (namely $s < q^n$), then $\sigma_q^{\pm}$ cannot drop by more than two, as in Example 7.1. We first need the following fact about "concatenating" nonnegative integers $s, d < q^n$ to form $sq^n + d$. We denote by $\mathcal{B}_s$ and $\mathcal{B}_d \subseteq \{0, \ldots, n-1\}$ the set of block indices from (5.1) for s and d, respectively.

LEMMA 7.2. *Let $q \geq 2$, $n \in \mathbf{N}$, $0 \leq d, s < q^n$. Then*

$$\sigma_q^{\pm}(sq^n + d) \leq \sigma_q^{\pm}(s) + \sigma_q^{\pm}(d) \leq \sigma_q^{\pm}(sq^n + d) + 2\,,$$

and if $0 \notin \mathcal{B}_s$, then

$$\sigma_q^{\pm}(s) + \sigma_q^{\pm}(d) \leq \sigma_q^{\pm}(sq^n + d) + 1\,.$$

PROOF. The first inequality follows from (4.4). For the second inequality, let $e = sq^n + d$, and denote by $\mathcal{B}_e$ and $\mathcal{D}_e \subseteq \{0, \ldots, 2n-1\}$ the set of block and bridge indices for e, as in (5.1) and (5.2), respectively. Let $\mathcal{C}_d, \mathcal{C}_s \subseteq \{0, \ldots, n-1\}$ be the set of bump indices for d, s, respectively.

We associate to each block $\{j, \ldots, k\}$ of s the interval $\{j+n, \ldots, k+n\}$, and to each block $\{j, \ldots, k\}$ of d the interval $\{j, \ldots, k\}$. Then we have associated to each block of s or d a block of e, except if $0 \in \mathcal{B}_s$ and $n-1 \in \mathcal{B}_d$, in which case two blocks are merged into one. Hence $\beta(s) + \beta(d) \leq \beta(e) + 1$, and $\beta(s) + \beta(d) = \beta(e)$ if

$$0 \notin \mathcal{B}_s \text{ or } n-1 \notin \mathcal{B}_d. \tag{7.1}$$

Similarly, we can associate to each bump of s or d a bump of e, except possibly for a "border conflict" at $n-1$ or n. Thus $\gamma(s)+\gamma(d) \le \gamma(e)+2$, and $\gamma(s)+\gamma(d)=\gamma(e)$ if

$$(0 \notin \mathcal{C}_s \text{ or } n-1 \notin \mathcal{B}_d \cup \mathcal{C}_d) \text{ and } (0 \notin \mathcal{B}_s \cup \mathcal{C}_s \text{ or } n-1 \notin \mathcal{C}_d). \tag{7.2}$$

In the same vein, we have $\delta(s)+\delta(d) \ge \delta(e)-1$, and $\delta(s)+\delta(d)=\delta(e)$ if

$$n \notin \mathcal{D}_e \text{ and } n-1 \notin \mathcal{D}_e. \tag{7.3}$$

Note that $\mathcal{B}_s \cap \mathcal{C}_s = \mathcal{B}_d \cap \mathcal{C}_d = \emptyset$. If (7.1) is not satisfied, then $0 \in \mathcal{B}_s$ and $n-1 \in \mathcal{B}_d$, and (7.2) and (7.3) hold. Similarly, the negation of (7.2) implies that $n, n-1 \in \mathcal{B}_e$ and (7.3). Lastly, $\tau(s)+\tau(d)=\tau(e)$. Thus

$$\begin{aligned} \sigma_q^{\pm}(s)+\sigma_q^{\pm}(d) &= \tau(s)+2\beta(s)+\gamma(s)-\delta(s)+\tau(d)+2\beta(d)+\gamma(d)-\delta(d) \\ &\le \tau(e)+2\beta(e)+\gamma(e)-\delta(e)+2 \\ &= \sigma_q^{\pm}(e)+2. \end{aligned}$$

This proves the first claim.

If $0 \notin \mathcal{B}_s$, we can have equality in the second inequality only if $\gamma(s)+\gamma(d)=\gamma(e)+2$. But then $\beta(s)+\beta(d)=\beta(e)-1$ and (7.3) holds, so that $\sigma_q^{\pm}(s)+\sigma_q^{\pm}(d)=\sigma_q^{\pm}(sq^n+d)$. This proves the second claim. □

THEOREM 7.3. *Let $q \ge 2$, $n \in \mathbb{N}$, $0 \le e, s < q^n$. Then*

$$\sigma_q^{\pm}(e+s(q^n-1)) \ge \sigma_q^{\pm}(e)-2.$$

PROOF. Set $d=e+s(q^n-1)$, and write $d=d_1q^n+d_0$ with $0 \le d_0, d_1 < q^n$. Then

$$e=d-s(q^n-1)=(d_1-s)q^n+d_0+s<q^n.$$

Since $d_0+s<2q^n$, we have $d_1-s=0$ or $d_1-s+1=0$. First suppose that $d_1=s$. Then $e=d_0+s$, and by (4.4) and Lemma 7.2, we have

$$\sigma_q^{\pm}(e) \le \sigma_q^{\pm}(d_0)+\sigma_q^{\pm}(s) \le \sigma_q^{\pm}(sq^n+d_0)+2=\sigma_q^{\pm}(d)+2.$$

Now suppose that $d_1+1=s$. Then $q^n+e=d_0+s$, and if $q \ge 3$, then

$$\begin{aligned} \sigma_q^{\pm}(e)+1 &= \sigma_q^{\pm}(q^n+e) \le \sigma_q^{\pm}(d_0)+\sigma_q^{\pm}(s) \\ &\le \sigma_q^{\pm}(d_0)+\sigma_q^{\pm}(d_1)+\sigma_q^{\pm}(1) \\ &\le \sigma_q^{\pm}(d_1q^n+d_0)+2+1. \end{aligned}$$

For $q = 2$, the first equality may fail to hold, since $\sigma_2^{\pm}(e) = \sigma_2^{\pm}(2^n + e)$ is possible. But then either d_1 is odd, in which case $0 \notin \mathcal{B}_{d_1}$ and $\sigma_2^{\pm}(s) \leq \sigma_2^{\pm}(d_1)$, or d_1 is even, in which case $\sigma_2^{\pm}(d_0) + \sigma_2^{\pm}(d_1) \leq \sigma_2^{\pm}(d_1 2^n + d_0) + 1$, by the second part of Lemma 7.2. In either case, we conclude that $\sigma_q^{\pm}(d) \geq \sigma_q^{\pm}(e) - 2$. □

It remains open whether $\sigma_q^{\pm}(e + s(q^n - 1)) \geq \sigma_q^{\pm}(e) - 2$ for any $s \in \mathbf{Z}$. The method above will show that $\sigma_q^{\pm}(e + s(q^n - 1)) \geq \sigma_q^{\pm}(e) - 2i$ if $s < q^{in}$.

Acknowledgements

Part of this work was done while the author was a Visiting Fellow at the Computer Sciences Laboratory, Australian National University, Canberra, Australia, and partly supported by Natural Sciences and Engineering Research Council of Canada, grant A2514. An Extended Abstract appeared in Proc. 32nd IEEE Symp. Found. of Computer Science, San Juan PR, 1991, 384–391.

References

G. B. Agnew, R. C. Mullin, and S. A. Vanstone, Fast exponentiation in $GF(2^n)$. In *Advances in Cryptology—EUROCRYPT '88*, ed. C. G. Günther, vol. 330 of *Lecture Notes in Computer Science*. Springer (Berlin), 1988, 251–255.

J. Berstel and S. Brlek, On the length of word chains. *Inform. Process. Lett.* **26** (1987), 23–28.

T. Beth, B. M. Cook, and D. Gollmann, Architectures for exponentiation in $GF(2^n)$. In *Advances in Cryptology—CRYPTO '86*, ed. A. M. Odlyzko, vol. 263 of *Lecture Notes in Computer Science*. Springer (Berlin), 1986, 302–310.

F. Fich and M. Tompa, The parallel complexity of exponentiating polynomials over finite fields. *J. Assoc. Comput. Mach.* **35** (1988), 651–667.

J. von zur Gathen, Computing powers in parallel. *SIAM J. Comput.* **16** (1987), 930–945.

J. von zur Gathen, Inversion in finite fields using logarithmic depth. *J. Symb. Comp.* **9** (1990), 175–183.

J. von zur Gathen, Processor-efficient exponentiation in finite fields. Inform. Process. Lett., to appear, 1992.

J. von zur Gathen and M. Giesbrecht, Constructing normal bases in finite fields. *J. Symb. Comp.* **10** (1990), 547–570.

J. von zur Gathen and G. Seroussi, Boolean circuits versus arithmetic circuits. *Inform. and Comput.* **91** (1991), 142–154.

P. N. Golovanov and V. I. Solodovnikov, Rapid parallel calculation of degrees in a quotient ring of polynomials over a finite field. *Mathematical Notes* **42** (1987), 987–992.

D. E. Knuth, *The Art of Computer Programming, Vol.2, Seminumerical Algorithms.* Addison-Wesley (Reading MA), 2 edition, 1981.

Th. Lengauer and K. Mehlhorn, VLSI complexity, efficient VLSI algorithms and the HILL design system. In *Algorithmics for VLSI*, ed. C. Trullemans. Academic Press, 1986, 33–89.

G. W. Reitwiesner, Binary arithmetic. *Advances in computers, ed. F. L. Alt* **1** (1960), 231–308.

D. R. Stinson, Some observations on parallel algorithms for fast exponentiation in $GF(2^n)$. *SIAM J. Comput.* **19** (1990), 711–717.

C. C. Wang, T. K. Truong, H. M. Shao, L. J. Deutsch, J. K. Omura, and I. S. Reed, VLSI architectures for computing multiplications and inverses in $GF(2^m)$. *IEEE Trans. Comput.* **C-34** (1985), 709–717.

Manuscript received 29 April 1991

Joachim von zur Gathen
Department of Computer Science
University of Toronto
Toronto, Ontario M5S 1A4, Canada
gathen@theory.toronto.edu