

Measuring With Jugs

Or

What If Mathematicians Were Asked To Defuse Bombs

Paolo Boldi* Massimo Santini* Sebastiano Vigna*
Dipartimento di Scienze dell'Informazione, Università degli Studi di Milano, Italy
{boldi,santini,vigna}@dsi.unimi.it

Script

COMPUTER: I am a bomb, you have just armed me.
SIMON GRUBER (*over a cellular phone*): I got you see the message. It has a proximity circuit, so please don't try to run.
JOHN MCCLANE: Yeah I got it. We're not gonna run. How do we turn this thing off?
SIMON: On the fountain, there should be two jugs. You see them, a five gallon jug and a three gallon jug? Fill one of the jugs with exactly four gallons of water and place it on the scale and the timer will stop. You must be precise. One ounce more or less will result in detonation. If you are still alive in five mins. . .
JOHN: Wait. . . wait a second. I don't get it, you get it?
ZEUS CARVER: No.
JOHN: Get the jugs. Obviously we can't fill the three gallon jug with four gallons of water, right?
ZEUS: Right.
JOHN: All right. I know. . . Here we go. We fill the three gallon jug exactly to the top. Right?
ZEUS: Uh huh.
JOHN: Okay. Now. We pour that three gallons in the five gallon jug, giving us exactly three gallons in the five gallon jug, right?
ZEUS: Right.
JOHN: Now, take the three gallon jug, fill that a third of the way up. . .
ZEUS: NO! He said precise. Exactly four gallons.

(Excerpt from *Die Hard 3*, a.k.a. *Die Hard: With a Vengeance*)

As in any typical Hollywood action movie, John and Zeus (smart guys, indeed) have been eventually able to defuse Simon's bomb. But next time, it could be (die) harder! So it is high time for three wanna-be mathematicians to help our heroes to save their skin, and solve their problem in a far more general setting.

Suppose we are given n initially empty jugs, each with a specified positive integer capacity c_i ; we can assume without loss of generality that $\mathbf{c} = (c_1, c_2, \dots, c_n)$ is an ordered vector (i.e., $c_1 \leq c_2 \leq \dots \leq c_n$), fixed from now onwards. We can perform three *elementary operations* (or *steps*) on the jugs, viz.:

*The authors have been partially supported by the ESPRIT Working Group EP 27150, Neural and Computational Learning II (NeuroCOLT II).

1. $\downarrow i$: fill the i -th jug (up to its capacity);
2. $i \uparrow$: empty the i -th jug;
3. $i \rightarrow j$: completely pour the content of the i -th jug into the j -th jug ($i \neq j$); at the end of this operation the i -th jug is empty or the j -th jug is full.

These operations can be formally described as follows. Let O denote the set of elementary operations; a *state* is a vector $s \in \mathbf{N}^n$, where s_i denotes the amount contained in jug i . The *next-state function* $\delta : \mathbf{N}^n \times O \rightarrow \mathbf{N}^n$ is defined as follows:

1. $\delta(s, \downarrow i) = (s_1, \dots, s_{i-1}, c_i, s_{i+1}, \dots, s_n)$;
2. $\delta(s, i \uparrow) = (s_1, \dots, s_{i-1}, 0, s_{i+1}, \dots, s_n)$;
3. $\delta(s, i \rightarrow j) = (t_1, \dots, t_n)$, where $t_k = s_k$ for all $k \notin \{i, j\}$, $t_i = \max(0, s_i - (c_j - s_j))$ and $t_j = \min(c_j, s_i + s_j)$. For sake of simplicity, we define $i \rightarrow i$ as an operation with no effect.

An *algorithm* is a finite sequence of elementary operations; the function δ is extended to algorithms $\sigma \in O^*$ in the usual way, i.e., $\delta(s, \varepsilon) = s$ and $\delta(s, \sigma o) = \delta(\delta(s, \sigma), o)$. A quantity $x \in \mathbf{N}$ is *measurable* (via the algorithm σ) iff one of the components of $\delta(\mathbf{0}, \sigma)$ is equal to x . The set of quantities which are measurable using the capacities in c is denoted by $M(c)$.

1 Fair challenges: What is measurable?

We are blessed with a sort of twisted fairness—we would never let Simon challenge John and Zeus to defuse an indefusable bomb. But to do this, we need to know what is measurable and what is not. On the other hand, we would like to help John and Zeus by giving them a universal bomb-defusing algorithm (even if they are not likely to know what the last word means).

For each $A \subseteq \mathbf{Z}$, let $\langle A \rangle$ denote the subgroup of $(\mathbf{Z}, +)$ generated by A (which is just the cyclic subgroup generated by $\gcd A$). Given $x \in \langle c_1, \dots, c_n \rangle$, there exists (possibly more than) one vector $\mathbf{x} = (x_1, \dots, x_n) \in \mathbf{Z}^n$ such that $x = \mathbf{x} \cdot \mathbf{c} = \sum_i x_i c_i$; any such vector \mathbf{x} will be called a *representation* of x (with respect to \mathbf{c}). We shall denote by $\|\mathbf{x}\|_1$ the ℓ_1 -norm of \mathbf{x} , i.e., $\|\mathbf{x}\|_1 = \sum_i |x_i|$.

We shall now give an algorithm \mathcal{A} for measuring a quantity $x \in \langle c_1, \dots, c_n \rangle \cap [0, c_n]$; the algorithm depends on a representation $\mathbf{x} = (x_1, \dots, x_n)$ for x , and it can be recursively defined as follows:

1. if $x = 0$ then $\mathcal{A}(\mathbf{x})$ is the empty algorithm ε ;
2. if there exists an index i such that $x_i > 0$ and $x - c_i \geq 0$, then

$$\mathcal{A}(\mathbf{x}) = \mathcal{A}(x_1, \dots, x_i - 1, \dots, x_n) \quad \downarrow i \quad i \rightarrow n;$$

3. if there exists an index i such that $x_i < 0$ and $x + c_i \leq c_n$, then

$$\mathcal{A}(\mathbf{x}) = \mathcal{A}(x_1, \dots, x_i + 1, \dots, x_n) \quad n \rightarrow i \quad i \uparrow;$$

4. otherwise, let i and j be any indices such that $x_i > 0$ and $x_j < 0$; then

$$\mathcal{A}(\mathbf{x}) = \mathcal{A}(x_1, \dots, x_i - 1, \dots, x_j + 1, \dots, x_n) \quad n \rightarrow j \quad \downarrow i \quad i \rightarrow j \quad j \uparrow \quad i \rightarrow n.$$

Note that \mathcal{A} is defined non-deterministically, but it is trivial to obtain a deterministic version of it. We now show that \mathcal{A} is indeed correct.

Lemma 1 Let $\mathbf{x} = (x_1, \dots, x_n)$ be a representation (w.r.t. \mathbf{c}) of $x \in \langle c_1, \dots, c_n \rangle \cap [0, c_n]$.

- (i). $\mathcal{A}(\mathbf{x})$ is well-defined;
- (ii). the algorithm $\mathcal{A}(\mathbf{x})$ performs at most $\frac{5}{2}\|\mathbf{x}\|_1$ elementary operations;
- (iii). x is measurable via $\mathcal{A}(\mathbf{x})$; more precisely, $\delta(\mathbf{0}, \mathcal{A}(\mathbf{x})) = (0, 0, \dots, 0, x)$.

Proof. (i). Firstly, notice that every recursive call to \mathcal{A} reduces $\|\mathbf{x}\|_1$ by one in cases (2) and (3), or by two in case (4), so recursion is well founded. Moreover, if cases (1)–(3) fail, then at least one index i satisfies $x_i > 0$ (for otherwise $x < 0$) and one index j satisfies $x_j < 0$ (for otherwise condition (2) would hold), so we end up in case (4), and the algorithm is defined for every \mathbf{x} .

We have to show that the condition $0 \leq \mathbf{x} \cdot \mathbf{c} \leq c_n$ is satisfied in the recursive calls to \mathcal{A} : this is certainly true for cases (2) and (3). As for case (4), we must show that $x + c_j - c_i \in [0, c_n]$: if $x + c_j - c_i < 0$ then $x + c_j < c_i \leq c_n$, and this is impossible—since $x_j < 0$, we would be in case (3); if $x + c_j - c_i > c_n$ then $x - c_i > c_n - c_j \geq 0$, and this is impossible—since $x_i > 0$, we would be in case (2).

(ii). Straightforward: in cases (2) and (3), $\|\mathbf{x}\|_1$ is reduced by one, and two operations are added; in case (4), $\|\mathbf{x}\|_1$ is reduced by two, and five operations are added.

(iii). By induction on $\|\mathbf{x}\|_1$. If $\|\mathbf{x}\|_1 = 0$, the result is trivial. For the inductive step, we distinguish three cases:

- in case (2), we have $\delta(\mathbf{0}, \mathcal{A}(\mathbf{x})) = \delta((0, \dots, 0, x - c_i), \downarrow i \rightarrow n)$, which is in turn equal to $\delta((0, \dots, c_i, 0, \dots, x - c_i), i \rightarrow n) = (0, \dots, 0, x)$;
- in case (3), we have $\delta(\mathbf{0}, \mathcal{A}(\mathbf{x})) = \delta((0, \dots, 0, x + c_i), n \rightarrow i \rightarrow i \uparrow)$, which is equal to $\delta((0, \dots, c_i, 0, \dots, x), i \uparrow) = (0, \dots, 0, x)$;
- in case (4), we have $\delta(\mathbf{0}, \mathcal{A}(\mathbf{x})) = \delta((0, \dots, 0, x - c_i + c_j), n \rightarrow j \rightarrow \downarrow i \rightarrow j \rightarrow j \uparrow \rightarrow i \rightarrow n)$. Note that $x - c_i + c_j \leq c_j$ (for otherwise $x - c_i > 0$) and $c_j - (x - c_i + c_j) \leq c_i$ (for otherwise $c_j - (x - c_i + c_j) > c_i$, which implies $x < 0$). This yields the following sequence of states: $(0, \dots, 0, x - c_i + c_j) \rightsquigarrow (0, \dots, 0, \dots, x - c_i + c_j, \dots, 0) \rightsquigarrow (0, \dots, c_i, \dots, x - c_i + c_j, \dots, 0) \rightsquigarrow (0, \dots, c_i - (c_j - (x - c_i + c_j)) = x, \dots, c_j, \dots, 0) \rightsquigarrow (0, \dots, x, \dots, 0, \dots, 0) \rightsquigarrow (0, \dots, 0, x)$. ■

Since it is trivial to observe that $M(\mathbf{c}) \subseteq \langle c_1, \dots, c_n \rangle \cap [0, c_n]$, we can state our first result as follows:

Theorem 1 $M(\mathbf{c}) = \langle c_1, \dots, c_n \rangle \cap [0, c_n]$.

This theorem can be used in very different ways: Simon can nastily choose a non-measurable quantity to let his enemies blow up; on the other hand, John and Zeus can decide without fail if it is time to say their last prayers or readily start the sequence of steps which will defuse the bomb.

2 It's a matter of time: The complexity of measurement

Heroes and foes are naturally interested in time. Mathematically speaking, they want to obtain upper and lower bounds for the complexity of measurement. For instance, Lemma 1 contains more information than Theorem 1—it also states that John and Zeus can possibly save their skin performing at most $\frac{5}{2}\|x\|_1$ steps. Can wanna-be mathematicians say anything more precise? Denote with $\mu(x)$ the least ℓ_1 -norm of a representation of x (w.r.t. \mathbf{c}); in other words, define

$$\mu(x) = \min_{\mathbf{x} \cdot \mathbf{c} = x} \|\mathbf{x}\|_1.$$

The map μ enjoys a number of properties (in fact, it is almost¹ a norm):

Lemma 2 Let $x, y \in \langle c_1, \dots, c_n \rangle$ and $h \in \mathbf{Z}$. Then:

- (i). $\mu(x) \geq 0$, and $\mu(x) = 0$ iff $x = 0$;
- (ii). $\mu(hx) \leq |h|\mu(x)$;
- (iii). $\mu(x + y) \leq \mu(x) + \mu(y)$;
- (iv). $\mu(c_i) = 1$, for all $1 \leq i \leq n$.

Proof. We prove just the third claim (the other ones being straightforward). If \mathbf{x} and \mathbf{y} are representations of x and y , respectively, we have $(\mathbf{x} + \mathbf{y}) \cdot \mathbf{c} = \mathbf{x} \cdot \mathbf{c} + \mathbf{y} \cdot \mathbf{c} = x + y$; so $\mathbf{x} + \mathbf{y}$ is a representation of $x + y$. Thus $\mu(x + y) \leq \min\{\|\mathbf{x} + \mathbf{y}\|_1 \mid \mathbf{x} \cdot \mathbf{c} = x \text{ and } \mathbf{y} \cdot \mathbf{c} = y\} \leq \min_{\mathbf{x} \cdot \mathbf{c} = x} \|\mathbf{x}\|_1 + \min_{\mathbf{y} \cdot \mathbf{c} = y} \|\mathbf{y}\|_1 = \mu(x) + \mu(y)$. ■

Armed with this new definition, we are now able to suggest to John and Zeus our first upper bound, which immediately follows from Lemma 1:

Theorem 2 Every $x \in M(\mathbf{c})$ can be measured in at most $\frac{5}{2}\mu(x)$ steps.

Life would be too easy, and Simon would be really unhappy, if by ingenuity John and Zeus could measure every quantity in $M(\mathbf{c})$ using a very small number of steps. But this is not true: we are going to show that at least $\frac{1}{2}\mu(x)$ steps are needed for measuring x (so the bound of the previous theorem is optimal up to a small multiplicative constant).

Lemma 3 Let o be an elementary operation, and s, s' be two states such that $\delta(s, o) = s'$. Then

$$\sum_i \mu(s_i) \leq \sum_i \mu(s'_i) + 2.$$

Proof. If $o = i \uparrow$ or $o = i \downarrow$ the result is immediate (we obtain $\mu(s'_i) = 0$ and $\mu(s'_i) = 1$, respectively). Suppose $o = i \rightarrow j$, and consider two cases: if $s_i \leq c_j - s_j$ then $s'_i = 0$ and $s'_j = s_j + s_i$, hence $\mu(s'_i) + \mu(s'_j) = \mu(s_j + s_i) \leq \mu(s_i) + \mu(s_j)$. If $s_i > c_j - s_j$ then $s'_j = c_j$ and $s'_i = s_i + s_j - c_j$; thus, $\mu(s'_i) + \mu(s'_j) = \mu(s_i + s_j - c_j) + \mu(c_j) \leq \mu(s_i) + \mu(s_j) + 2$. ■

Theorem 3 No algorithm can measure $x \in M(\mathbf{c})$ in less than $\frac{1}{2}\mu(x)$ steps.

¹We remark that in general equality does not hold in the second claim of Lemma 2: indeed, for $\mathbf{c} = (2, 3)$ we have $3(-1, 1) \cdot \mathbf{c} = (0, 1) \cdot \mathbf{c}$, so $1 = \mu(3) < 3\mu(1)$.

Proof. Let σ be an algorithm which measures x , i.e., $\delta(\mathbf{0}, \sigma) = s$, and $s_i = x$ for some i . The claim is proved observing that $\mu(x) = \mu(s_i) \leq \sum_j \mu(s_j)$, which is at most twice the number of steps of σ . ■

If mathematicians had some time for experimental analysis, they could obtain for **Fun** the diagram of Figure 1, which shows the upper and lower bounds (dotted lines) of Theorem 2 and Theorem 3 in the case $\mathbf{c} = (15, 21, 35)$, together with the number of steps of the optimal algorithm (solid line): the latter has been computed by exhaustive search.

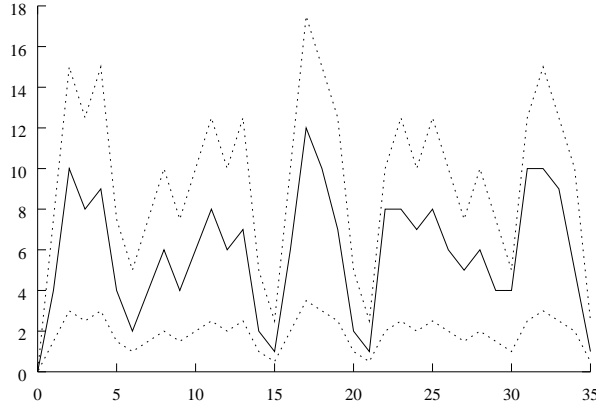


Figure 1: The case $\mathbf{c} = (15, 21, 35)$.

2.1 Hinting at John and Zeus: An upper bound for μ

The bound of Theorem 2 is not particularly meaningful to John and Zeus, so we would like to give them an explicit upper bound for μ . Let $\mathbf{a} \in \mathbb{N}^n$, $\mathbf{b} \in \mathbb{N}^m$ be the coefficients of the *linear homogeneous Diophantine equation* $\sum_i a_i y_i - \sum_j b_j z_j = 0$ in the indeterminates $\mathbf{y} \in \mathbb{N}^n$, $\mathbf{z} \in \mathbb{N}^m$ and call $S(\mathbf{a}, \mathbf{b})$ the submonoid of \mathbb{N}^{n+m} of all its solutions, i.e.,

$$S(\mathbf{a}, \mathbf{b}) = \{(\mathbf{y}, \mathbf{z}) \in \mathbb{N}^{n+m} \mid \sum_i a_i y_i - \sum_j b_j z_j = 0\};$$

the *Hilbert basis* $S_{\min}(\mathbf{a}, \mathbf{b}) \subset S(\mathbf{a}, \mathbf{b})$ is the set of all minimal nontrivial solutions of the equation, with respect to the componentwise ordering (see [GP79]).

Lemma 4 ([Lam87]) The monoid $S(\mathbf{a}, \mathbf{b})$ is generated by $S_{\min}(\mathbf{a}, \mathbf{b})$, which is of finite cardinality; for any solution $(\mathbf{y}, \mathbf{z}) \in S_{\min}(\mathbf{a}, \mathbf{b})$, $\|\mathbf{y}\|_1 \leq \max_j b_j$ and $\|\mathbf{z}\|_1 \leq \max_i a_i$.

As a consequence, it is possible to prove the following

Theorem 4 Let $x \in \langle c_1, \dots, c_n \rangle$; then $\mu(x) < \max(2c_n, c_n + |x|) / \gcd(c_1, \dots, c_n)$.

Proof. Assume without loss of generality that $x > 0$ and consider an arbitrary representation \mathbf{x} of x . Define $I = \{i \mid x_i \geq 0\}$, $J = \{j \mid x_j < 0\}$, and let $d = \gcd(c_1, \dots, c_n)$. Then the Diophantine equation

$$\sum_{i \in I} y_i \frac{c_i}{d} - \sum_{j \in J} z_j \frac{c_j}{d} - w \frac{x}{d} = 0$$

(in the indeterminates y_i, z_j, w) has a solution with $w = 1$ (just set $y_i = x_i$ for $i \in I$, $z_j = -x_j$ for $j \in J$). In force of the previous lemma, there is a minimal solution $(\bar{y}, \bar{z}, 1)$ satisfying

$$\sum_{i \in I} \bar{y}_i \leq \max \left(\max_{j \in J} \frac{c_j}{d}, \frac{x}{d} \right) \quad \text{and} \quad 1 + \sum_{j \in J} \bar{z}_j \leq \max_{i \in I} \frac{c_i}{d}.$$

By memberwise adding these inequalities we obtain the result. ■

Forgetting our heroes for a moment, it is interesting to remark that μ induces a distance between natural numbers, by the standard definition $d(x, y) = \mu(x - y)$ (when x is not in $\langle c_1, \dots, c_n \rangle$, $\mu(x)$ is infinite). This distance has a graph-theoretical interpretation—it is the distance between x and y in the undirected Cayley graph Γ of \mathbf{Z} with respect to c_1, \dots, c_n ; thus, the upper bound of the previous theorem provides upper bounds for the distances of Γ as well. Moreover, getting back to our story, it allows us to give an upper bound for measurement which does not involve μ :

Corollary 1 Every $x \in M(c)$ can be measured in at most $5c_n / \gcd(c_1, \dots, c_n)$ steps.

3 Dying harder and harder: Real capacities and density

It may not be so self-evident, but Simon could be extremely nastier than he is—he could use jugs with arbitrary capacities! Yet, it is not difficult to check that Theorem 1 holds also when the capacities c_i are positive real numbers², and $\langle c_1, \dots, c_n \rangle$ denotes the subgroup of $(\mathbf{R}, +)$ generated by c_1, \dots, c_n . Moreover, a simple scale-changing argument proves the following

Theorem 5 For all $0 < \alpha \in \mathbf{R}$ and $c \in \mathbf{R}^n$, $M(\alpha c) = \alpha M(c)$.

If all ratios c_i/c_j are rational, each capacity is just an integer multiple of a certain $\alpha > 0$ (in particular, this happens if c is rational). The situation in this case is completely characterized: since the previous theorem gives $M(c)$ in terms of $M(c/\alpha)$, and $c/\alpha \in \mathbf{N}^n$, we can use the results of the previous sections.

However, if at least one ratio $c_j/c_i = \xi$ is not rational, it is a straightforward consequence of Kronecker's Theorem [HW62, Theorem 440] that $M(c)$ is dense in $[0, c_n]$. In particular, it is possible to measure an *arbitrary capacity* in $[0, c_n]$ with *arbitrary precision*. So we now leave our heroes and foes to their destiny, and play a little bit with jugs and formulae (John and Zeus could never measure a quantity as suggested below—the mistakenly spilled water would largely exceed the measurement error!). In analogy with the discrete case, we can define

$$\mu_\varepsilon(x) = \min_{|x - c \cdot x| \leq \varepsilon} \|x\|_1,$$

for $x \in [0, c_n]$ and $\varepsilon \geq 0$; unfortunately μ_ε does not enjoy the properties of Lemma 2, unless $\varepsilon = 0$. However, the lower and upper bounds given by Theorems 2 and 3 immediately generalize:

Theorem 6 For every $\varepsilon > 0$, every $x \in [0, c_n]$ can be measured with precision ε in no less than $\frac{1}{2}\mu_\varepsilon(x)$ and no more than $\frac{5}{2}\mu_\varepsilon(x)$ steps.

²As a matter of fact, the algorithm \mathcal{A} can even be used when the capacities are taken from an arbitrary ordered group. Moreover, the characterization is true (with obvious modifications) even when the set of jugs is infinite. But this is material for *Die Hard n*, $n > 4 \dots$

Proof. Only the lower bound needs a proof. Note that if $|x - a| \leq \varepsilon$, with $a \in M(\mathbf{c})$, then $\mu_\varepsilon(x) \leq \mu_0(a)$ and Lemma 3 remains true if μ is replaced with μ_0 . Hence, using the same notation as in the proof of Theorem 3, $\mu_\varepsilon(x) \leq \mu_0(s_i)$, which is less than twice the number of steps of the algorithm measuring $a = s_i$. ■

Bounding μ_ε is of course much more difficult than bounding μ . We shall limit ourselves to the case in which ξ belongs to a very particular set: in order to do this, we need introduce some notations, definitions and lemmata from number theory. Let $a_0, a_1, a_2, \dots, a_N$ be integers such that $a_i > 0$ for all $i > 0$. Define the *simple (finite) continued fraction of partial quotients* a_0, \dots, a_N as follows

$$[a_0, \dots, a_N] = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\dots + \frac{1}{a_N}}}}.$$

Let now $p_{-1} = 1, q_{-1} = 0, p_0 = a_0, q_0 = 1$ and define, for $n = 0, \dots, N-1$, the *convergents*

$$p_{n+1} = a_{n+1}p_n + p_{n-1} \quad \text{and} \quad q_{n+1} = a_{n+1}q_n + q_{n-1}.$$

It can be easily shown [HW62, Theorems 149 and 157] that $\gcd(p_n, q_n) = 1$ and

$$[a_0, \dots, a_N] = \frac{p_N}{q_N}.$$

The notion of continued fraction can be generalized to the infinite case: if a_0, a_1, \dots are integers (with $a_i > 0$ for $i > 0$), define the *simple continued fraction of partial quotients* a_0, a_1, \dots as

$$[a_0, a_1, \dots] = \lim_{N \rightarrow \infty} [a_0, \dots, a_N].$$

It turns out [HW62, Theorem 170] that every irrational number ξ can be expressed in just one way as an infinite simple continued fraction $[a_0, a_1, \dots]$ (which will be called the *continued fraction expansion* of ξ); moreover, if $\xi > 0$ then $a_0 \geq 0$. Following common usage, we define

$$1 \leq K(\xi) = \sup_{n \geq 1} a_n,$$

and say that an irrational ξ has *bounded partial quotients* if $K(\xi) < \infty$; moreover, we let $\mathcal{B} = \{\xi \in \mathbf{R} \mid K(\xi) < \infty\}$. It can be shown that while \mathcal{B} has Lebesgue measure zero, and so it is totally disconnected, it has Hausdorff–Besicovitch dimension 1, so it is a “most fractal” set (for a thorough discussion of these and other related issues, see [Sha92]).

We start with our first lemma concerning continued fraction expansion:

Lemma 5 Let $\xi = [a_0, a_1, \dots] \in \mathcal{B} \setminus \mathbf{Q}$ be a positive irrational number with bounded partial quotients, with convergents p_n, q_n . Then, for all $n \in \mathbf{N}$ it holds that

$$F_n \leq q_n \leq (\phi K(\xi))^n \quad \text{and} \quad p_n \leq \lceil \xi \rceil (\phi K(\xi))^n.$$

where $\phi = \frac{1+\sqrt{5}}{2}$ is the *golden ratio*, and F_n is the n -th Fibonacci number.

Proof. We first prove the upper bound for p_n by induction on n (the proof for q_n is analogous). Note that $p_0 = a_0 < \lceil \xi \rceil$, $p_1 = a_0 a_1 + 1 \leq \lfloor \xi \rfloor \phi K(\xi) + \phi K(\xi) = \lceil \xi \rceil \phi K(\xi)$ and that

$$\begin{aligned} p_{n+1} &= a_{n+1} p_n + p_{n-1} \leq K(\xi) \lceil \xi \rceil (\phi K(\xi))^n + \lceil \xi \rceil (\phi K(\xi))^{n-1} \\ &= \lceil \xi \rceil (\phi K(\xi))^{n-1} (\phi K(\xi)^2 + 1). \end{aligned}$$

If it was $\phi K(\xi)^2 + 1 > \phi^2 K(\xi)^2$ we would have $(\phi^2 - \phi) K(\xi)^2 < 1$, so (since $\phi^2 - \phi = 1$), $K(\xi) < 1$, which is impossible. Thus, $\phi K(\xi)^2 + 1 \leq \phi^2 K(\xi)^2$, and we obtain the required result. For the lower bound, we have $q_0 = 1 = F_0$, $q_1 = a_1 \geq 1 = F_1$ and $q_{n+1} = a_{n+1} q_n + q_{n-1} \geq q_n + q_{n-1} \geq F_n + F_{n-1} = F_{n+1}$. ■

Using this lemma, we can obtain a special version (providing also an upper bound for the value of convergents) of Theorem 171 of [HW62]. Note that, since F_n is the integer closest to $\phi^n / \sqrt{5}$, we have $F_{\lceil \log_\phi(\sqrt{5}n) \rceil} \geq n$.

Lemma 6 Let $\xi \in \mathcal{B} \setminus \mathbf{Q}$. For each $M > 0$ there exist two coprime $r, q \in \mathbf{Z}$ such that $q \geq M$,

$$\left| \frac{r}{q} - \xi \right| < \frac{1}{q^2}$$

and $|r| + |q| \leq \lceil \xi + 1 \rceil \phi K(\xi) (\sqrt{5}M)^{1+\log_\phi K(\xi)}$.

Proof. Let $n = \lceil \log_\phi(\sqrt{5}M) \rceil$. The inequality above holds by Theorem 171 of [HW62], taking $r = p_n$ and $q = q_n$; note that $q_n \geq F_n \geq M$ as required. Finally, by Lemma 5, $|r| + |q| = |p_n| + |q_n| \leq (\phi K(\xi))^n + \lceil \xi \rceil (\phi K(\xi))^n \leq \lceil \xi + 1 \rceil (\phi K(\xi))^{\log_\phi(\sqrt{5}M)+1} = \lceil \xi + 1 \rceil \phi \sqrt{5} M K(\xi)^{\log_\phi(\sqrt{5}M)+1}$. An easy calculation leads to the stated result. ■

We then obtain the following special version of Kronecker's Theorem:

Theorem 7 Let $\xi \in \mathcal{B} \setminus \mathbf{Q}$, $\alpha \in \mathbf{R}$ and $N > 0$. There exist $n, p \in \mathbf{Z}$ such that $n \geq N$,

$$|n\xi - p - \alpha| < \frac{3}{n}$$

and $|n| + |p| \leq \frac{3}{2} \lceil \xi + 1 \rceil \phi K(\xi) (2\sqrt{5}N)^{1+\log_\phi K(\xi)} + |\alpha| + 1$.

Proof. By Lemma 6, there exist $r, q \in \mathbf{Z}$ coprime, with $q \geq 2N$, such that

$$\left| \frac{r}{q} - \xi \right| < \frac{1}{q^2}$$

and $|r| + |q| \leq \lceil \xi + 1 \rceil \phi K(\xi) (2\sqrt{5}N)^{1+\log_\phi K(\xi)}$.

Let now Q be (one of the two) integers which are closer to $q\alpha$; then $|q\alpha - Q| \leq 1/2$. Since r and q are coprime, Q may be expressed as $Q = vr - uq$ for some $v, u \in \mathbf{Z}$, and we may assume that $|v| \leq q/2$. Note that $uq = vr - Q$ and thus

$$|u| \leq \frac{|v||r| + |Q|}{q} \leq \frac{\frac{1}{2}q|r| + q|\alpha| + 1}{q} \leq \frac{|r|}{2} + |\alpha| + 1.$$

Now $v(q\xi - r) - (q\alpha - Q) = q(v\xi - \alpha - u)$, hence

$$|q(v\xi - \alpha - u)| = |v(q\xi - r) - (q\alpha - Q)| \leq |v||q\xi - r| + |q\alpha - Q| < \frac{1}{2}q \frac{1}{q} + \frac{1}{2} = 1.$$

Letting $n = q + v$ and $p = r + u$, we obtain

$$|n\xi - p - \alpha| = |q\xi + v\xi - r - u - \alpha| \leq |v\xi - u - \alpha| + |q\xi - r| < \frac{1}{q} + \frac{1}{q} = \frac{2}{q}.$$

Since $|v| \leq q/2$, we have $q/2 \leq q + v \leq (3/2)q$. Moreover $q \geq 2N$, which implies $N \leq q/2$, and so $N \leq q/2 \leq n \leq 3q/2$. Hence $2/q \leq n/3$, and we obtain the required bound. Finally,

$$|n| + |p| \leq |q| + |v| + |r| + |u| \leq q + \frac{1}{2}q + |r| + \frac{1}{2}|r| + |\alpha| + 1 = \frac{3}{2}(|q| + |r|) + |\alpha| + 1$$

which is at most $\frac{3}{2}[\xi + 1]\phi K(\xi)(2\sqrt{5}N)^{1+\log_\phi K(\xi)} + |\alpha| + 1$. ■

We now turn the previous theorem into an upper bound for μ_ε :

Theorem 8 Let $\mathbf{c} \in \mathbf{R}^n$ and assume $c_j/c_i = \xi$ for some irrational $\xi \in \mathcal{B} \setminus \mathbf{Q}$ with bounded partial quotients. Then, for each $x \in \mathbf{R}$ and each $\varepsilon > 0$

$$\mu_\varepsilon(x) \leq \frac{3}{2}[\xi + 1]\phi K(\xi) \left(\frac{6\sqrt{5}c_i}{\varepsilon} \right)^{1+\log_\phi K(\xi)} + \frac{x}{c_i} + 1.$$

Proof. Let $N = 3c_i/\varepsilon$ and $\alpha = x/c_i$. By Theorem 7, we find $n, p \in \mathbf{Z}$ such that $n \geq N$,

$$|n\xi - p - \alpha| < \frac{3}{n} \leq \frac{3}{N} = \frac{\varepsilon}{c_i}$$

and $|n| + |p| \leq \frac{3}{2}[\xi + 1]\phi K(\xi) \left(\frac{6\sqrt{5}c_i}{\varepsilon} \right)^{1+\log_\phi K(\xi)} + \frac{x}{c_i} + 1$. But $|nc_j - pc_i - \alpha c_i| = |n\xi c_i - pc_i - \alpha c_i| = c_i|n\xi - p - \alpha| < \varepsilon$. ■

This obviously can be combined with Theorem 6 in order to obtain an upper bound for the number of steps required to measure $x \in [0, c_n]$ with precision ε .

3.1 The special case $\mathbf{c} = (1, \phi)$

When ξ is the golden ratio (whose expansion is easily shown to be $[1, 1, 1, \dots]$), we have $K(\phi) = 1$ and thus the upper bound of Theorem 6, using Theorem 8, has the form

$$\kappa_1 \frac{1}{\varepsilon} + \kappa_2 x + 1$$

for appropriate constants κ_1 and κ_2 . The fact that ϕ is so well suited to measurement can be immediately related to its usefulness in *multiplicative hashing* [Knu97]. Every point of the sequence $\{t\phi\} = t\phi - \lfloor t\phi \rfloor$ on the unit interval bisects (following the golden ratio) one of the longest intervals not containing previous points [Šwi58], i.e., the sequence is “most uniformly distributed” (more precisely, this is true of ϕ^{-1} , but $\{t\phi^{-1}\} = \{t\phi\}$). This fact can be used in order to provide a lower bound for the case $\mathbf{c} = (1, \phi)$.

Lemma 7 At least one of the intervals determined on the unit interval by the set of points $\{\{t\phi\} \mid 0 \leq t < F_{n+1}\} \cup \{\{-t\phi\} \mid 0 \leq t < F_{n+1}\}$ has length greater than $\frac{1}{2}\phi^{-2n}$.

Proof. We use the fact that the point $\{k\phi\}$ bisects following the golden ratio one of the longest intervals determined by $\{\{t\phi\} \mid 0 \leq t < k\}$ on the unit interval, and that new lengths appear only when k is a Fibonacci number (see [Knu97] for a full discussion). Since each bisection

possibly reduces an interval by a factor of $1 - \phi^{-1} = \phi^{-2}$, all intervals determined by $\{t\phi \mid 0 \leq t < F_{n+1}\}$ have at least length ϕ^{-2n} (the same holds for the other set of points). Hence, the statement can be easily obtained observing that the union of the two sets must leave at least one segment of length greater than $\frac{1}{2}\phi^{-2n}$ (no point of a set can exactly bisect an interval determined by the other set). ■

Lemma 8 For all $n > 0$ there exists $x \in (0, 1)$ such that for all $p, t \in \mathbf{Z}$ with $|t| < n$, it holds

$$|t\phi + p - x| > \left(\frac{\phi}{2\sqrt{5}n}\right)^2.$$

Proof. Since $|t| < n \leq F_{\lceil \log_\phi(\sqrt{5}n) \rceil}$, by the previous lemma the set of points $\{t\phi + p \mid |t| < n, p \in \mathbf{Z}\} = \{t\phi\} + p \mid |t| < n, p \in \mathbf{Z}\}$ determines at least one interval of length greater than $\frac{1}{2}\phi^{-2\lceil \log_\phi(\sqrt{5}n) \rceil + 2} \geq \frac{1}{2}(\phi/\sqrt{5}n)^2$ in $[0, 1]$. Choosing x as its middle point, we obtain the thesis. ■

Now we can state a lower bound for μ_ε :

Theorem 9 For every $\varepsilon \in (0, 1)$ there exists an $x \in (0, 1)$ such that

$$\mu_\varepsilon(x) \geq \frac{2\phi + 1}{2\sqrt{5}\varepsilon} - \phi - 3.$$

Proof. Let $n = \lfloor \phi/(2\sqrt{5}\varepsilon) \rfloor$; then, by the previous lemma, a simple substitution shows that there exists $x \in (0, 1)$ such that for all $p, t \in \mathbf{Z}$ with $|t| < n$ it holds $|t\phi + p - x| > \varepsilon$. Thus, for every $\mathbf{x} \in \mathbf{Z}^2$ such that $|\mathbf{c} \cdot \mathbf{x} - x| \leq \varepsilon$ we have $|x_2| \geq n$. Moreover, $|x_1 + x_2\phi| \leq \varepsilon + x \leq 2$ and thus $|x_1| \geq |x_2|\phi - 2$, so $\|\mathbf{x}\|_1 \geq |x_2|(1 + \phi) - 2 \geq (n + 1)(1 + \phi) - \phi - 3$. ■

In other words, for some $x \in (0, 1)$ (in fact, on some positive measure subset of $[0, 1]$) μ_ε has a lower bound of the form

$$\kappa \frac{1}{\sqrt{\varepsilon}} - \phi - 3,$$

with constant $\kappa \approx 1$, a fact that we could use in order to design bombs with a guaranteed minimum defusing time (in fact, the right subtitle of this paper should be *What If Mathematicians Were Asked To Design Bombs...*).

4 Acknowledgements

We kindly thank Giuseppe “*u spaccafurnaru*” Melfi³ for the proof of the bound $\mu(x) \leq nc_n$, which we subsequently improved to Theorem 4. We also thank Jeffrey “Elvis-number-3” Shalilit⁴ for his thorough survey [Sha92], which he kindly and promptly FedEx’d us. Giovanni “Big Wednesday” Vigna and Sharon Webb provided the excerpt from the screenplay of *Die Hard: With a Vengeance*, which is Copyright © 1995 Twentieth–Century Fox. This paper was mainly written for the authors’ **FUN**, so we hope it will be **FUNNY** for someone else, too.

³Giuseppe is from Ispica, a small town in Sicily, whose name under the fascist dictatorship was changed in *Spaccafuorno*, literally “oven breaker”. The inhabitants of the nearby cities still call the people from Ispica *spaccafurnari* when speaking in dialect.

⁴Mathematicians count their distance from Paul Erdős; musicians count their distance from Elvis.

References

- [GP79] F. R. Giles and W. R. Pulleyblank. Total dual integrality and integer polyhedra. *Linear Algebra Appl.*, 25:191–196, 1979.
- [HW62] G.H. Hardy and E.M. Wright. *The Theory of Numbers*. Oxford University Press, fourth edition, 1962.
- [Knu97] Donald E. Knuth. *Sorting and Searching*, volume 3 of *The Art of Computer Programming*. Addison-Wesley, Reading, MA, USA, second edition, 1997.
- [Lam87] Jean-Luc Lambert. Une borne pour les générateurs des solutions entières positives d’une équation diophantienne linéaire. *Compte-rendus de l’Académie des Sciences de Paris*, 305(1):39–40, 1987.
- [Sha92] Jeffrey O. Shallit. Real numbers with bounded partial quotients: A survey. *Enseign. Math. (2)*, 38:151–187, 1992.
- [Świ58] Stanisław Świerczkowski. On successive settings of an arc on the circumference of a circle. *Fund. Math.*, 46:187–189, 1958.