Random Digit Representation of Integers

Nicolas Méloni (meloni@univ-tln.fr)
Université de Toulon

Fast exponentiation

Require: $k = (k_{l-1} \dots k_0)_2$, $k_i \in 0 \cup \{d_1, \dots, d_n\}$, g a group element

Ensure: g^k

1: $h \leftarrow 1$
2: compute $g^{d_1}, g^{d_2}, \dots, g^{d_n}$
3: **for** $i = l-1 \dots 0$ **do**
4: $\quad h \leftarrow h^2$
5: $\quad$ **if** $k_i \neq 0$ **then**
6: $\quad\quad h \leftarrow h \times g^{k_i}$
7: $\quad$ **end if**
8: **end for**
9: **return** h

Example: $\mathcal{D} = \{1, 2, 3\}$ $k = 314 = (100030202)_2$

- g, g^2, g^3
  $h = 1$
- g
- g^2, g^4, g^8
- g^{16}, g^{19}
- g^{38}
- g^{76}, g^{78}
- g^{156}
- g^{312}, g^{314}

N. Méloni
IMATH - Université de Toulon

Fast exponentiation

Require: $k = (k_{l-1} \dots k_0)_2$, $k_i \in 0 \cup \{d_1, \dots, d_n\}$, g a group element
Ensure: g^k

1: $h \leftarrow 1$
2: compute $g^{d_1}, g^{d_2}, \dots, g^{d_n}$
3: **for** $i = l-1 \dots 0$ **do**
4: $\quad h \leftarrow h^2$
5: $\quad$ **if** $k_i \neq 0$ **then**
6: $\quad\quad h \leftarrow h \times g^{k_i}$
7: $\quad$ **end if**
8: **end for**
9: **return** h

Example: $\mathcal{D} = \{1, 2, 3\}$ $k = 314 = (100030202)_2$

- g, g^2, g^3
  $h = 1$
- g
- g^2, g^4, g^8
- g^{16}, g^{19}
- g^{38}
- g^{76}, g^{78}
- g^{156}
- g^{312}, g^{314}

N. Méloni
IMATH - Université de Toulon

Fast exponentiation

Require: $k = (k_{l-1} \dots k_0)_2$, $k_i \in 0 \cup \{d_1, \dots, d_n\}$, g a group element

Ensure: g^k

1: $h \leftarrow 1$
2: compute $g^{d_1}, g^{d_2}, \dots, g^{d_n}$
3: **for** $i = l-1 \dots 0$ **do**
4: $\quad h \leftarrow h^2$
5: $\quad$ **if** $k_i \neq 0$ **then**
6: $\quad\quad h \leftarrow h \times g^{k_i}$
7: $\quad$ **end if**
8: **end for**
9: **return** h

Example: $\mathcal{D} = \{1, 2, 3\}$ $k = 314 = (100030202)_2$

- g, g^2, g^3
  $h = 1$
- g
- g^2, g^4, g^8
- g^{16}, g^{19}
- g^{38}
- g^{76}, g^{78}
- g^{156}
- g^{312}, g^{314}

N. Méloni
IMATH - Université de Toulon

Fast exponentiation

Require: $k = (k_{l-1} \dots k_0)_2$, $k_i \in 0 \cup \{d_1, \dots, d_n\}$, g a group element

Ensure: g^k

1: $h \leftarrow 1$
2: compute $g^{d_1}, g^{d_2}, \dots, g^{d_n}$
3: **for** $i = l-1 \dots 0$ **do**
4: $\quad h \leftarrow h^2$
5: $\quad$ **if** $k_i \neq 0$ **then**
6: $\quad\quad h \leftarrow h \times g^{k_i}$
7: $\quad$ **end if**
8: **end for**
9: **return** h

Example: $\mathcal{D} = \{1, 2, 3\}$ $k = 314 = (100030202)_2$

- g, g^2, g^3
  $h = 1$
- g
- g^2, g^4, g^8
- g^{16}, g^{19}
- g^{38}
- g^{76}, g^{78}
- g^{156}
- g^{312}, g^{314}

N. Méloni
IMATH - Université de Toulon

Fast exponentiation

Require: $k = (k_{l-1} \dots k_0)_2$, $k_i \in 0 \cup \{d_1, \dots, d_n\}$, g a group element

Ensure: g^k

1: $h \leftarrow 1$
2: compute $g^{d_1}, g^{d_2}, \dots, g^{d_n}$
3: **for** $i = l-1 \dots 0$ **do**
4: $\quad h \leftarrow h^2$
5: $\quad$ **if** $k_i \neq 0$ **then**
6: $\quad\quad h \leftarrow h \times g^{k_i}$
7: $\quad$ **end if**
8: **end for**
9: **return** h

Example: $\mathcal{D} = \{1, 2, 3\}$ $k = 314 = (100030202)_2$

- g, g^2, g^3
  $h = 1$
- g
- g^2, g^4, g^8
- g^{16}, g^{19}
- g^{38}
- g^{76}, g^{78}
- g^{156}
- g^{312}, g^{314}

N. Méloni
IMATH - Université de Toulon

Fast exponentiation

Require: $k = (k_{l-1} \dots k_0)_2$, $k_i \in 0 \cup \{d_1, \dots, d_n\}$, g a group element

Ensure: g^k

1: $h \leftarrow 1$
2: compute $g^{d_1}, g^{d_2}, \dots, g^{d_n}$
3: **for** $i = l-1 \dots 0$ **do**
4: $\quad h \leftarrow h^2$
5: $\quad$ **if** $k_i \neq 0$ **then**
6: $\quad\quad h \leftarrow h \times g^{k_i}$
7: $\quad$ **end if**
8: **end for**
9: **return** h

Example: $\mathcal{D} = \{1, 2, 3\}$ $k = 314 = (100030202)_2$

- g, g^2, g^3
  $h = 1$
- g
- g^2, g^4, g^8
- g^{16}, g^{19}
- g^{38}
- g^{76}, g^{78}
- g^{156}
- g^{312}, g^{314}

N. Méloni
IMATH - Université de Toulon

Fast exponentiation

Require: $k = (k_{l-1} \dots k_0)_2$, $k_i \in 0 \cup \{d_1, \dots, d_n\}$, g a group element
Ensure: g^k

1: $h \leftarrow 1$
2: compute $g^{d_1}, g^{d_2}, \dots, g^{d_n}$
3: **for** $i = l-1 \dots 0$ **do**
4: $\quad h \leftarrow h^2$
5: $\quad$ **if** $k_i \neq 0$ **then**
6: $\quad\quad h \leftarrow h \times g^{k_i}$
7: $\quad$ **end if**
8: **end for**
9: **return** h

Example: $\mathcal{D} = \{1, 2, 3\}$ $k = 314 = (100030202)_2$

- g, g^2, g^3
  $h = 1$
- g
- g^2, g^4, g^8
- g^{16}, g^{19}
- g^{38}
- g^{76}, g^{78}
- g^{156}
- g^{312}, g^{314}

N. Méloni
IMATH - Université de Toulon

Fast exponentiation

Require: $k = (k_{l-1} \dots k_0)_2$, $k_i \in 0 \cup \{d_1, \dots, d_n\}$, g a group element

Ensure: g^k

1: $h \leftarrow 1$
2: compute $g^{d_1}, g^{d_2}, \dots, g^{d_n}$
3: **for** $i = l-1 \dots 0$ **do**
4: $\quad h \leftarrow h^2$
5: $\quad$ **if** $k_i \neq 0$ **then**
6: $\quad\quad h \leftarrow h \times g^{k_i}$
7: $\quad$ **end if**
8: **end for**
9: **return** h

Example: $\mathcal{D} = \{1, 2, 3\}$ $k = 314 = (100030202)_2$

- g, g^2, g^3
  $h = 1$
- g
- g^2, g^4, g^8
- g^{16}, g^{19}
- g^{38}
- g^{76}, g^{78}
- g^{156}
- g^{312}, g^{314}

N. Méloni
IMATH - Université de Toulon

Fast exponentiation

Require: $k = (k_{l-1} \dots k_0)_2$, $k_i \in 0 \cup \{d_1, \dots, d_n\}$, g a group element
Ensure: g^k

1: $h \leftarrow 1$
2: compute $g^{d_1}, g^{d_2}, \dots, g^{d_n}$
3: **for** $i = l-1 \dots 0$ **do**
4: $\quad h \leftarrow h^2$
5: $\quad$ **if** $k_i \neq 0$ **then**
6: $\quad\quad h \leftarrow h \times g^{k_i}$
7: $\quad$ **end if**
8: **end for**
9: **return** h

Example: $\mathcal{D} = \{1, 2, 3\}$ $k = 314 = (100030202)_2$

- g, g^2, g^3
  $h = 1$
- g
- g^2, g^4, g^8
- g^{16}, g^{19}
- g^{38}
- g^{76}, g^{78}
- g^{156}
- g^{312}, g^{314}

N. Méloni
IMATH - Université de Toulon

Fast exponentiation

- Less digits, less precomputations
- More zeros, less computations
  - $k = (100111010)_2 \rightarrow$, 4 mult, no precomp
  - $k = (100030202)_2 \rightarrow$, 3 mult + 2 mult precomp
  - $k = (100007002)_2 \rightarrow$, 2 mult + 4-6 mult precomp
- We are interested in
  - the size of $\mathcal{D}$ (number of digits)
  - the density of the representation (average number of zeros)
  - how to compute the representation!

Integer recoding in a nutshell

Let $k = 31415$

$\mathcal{D} = \{1\}$

$$
\begin{array}{rcccccccccccccccc}
k & = & & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\
& = & & & & 7 & 0 & 0 & 5 & 0 & 0 & 2 & 0 & 0 & 6 & 0 & 0 & 7 \\
& = & & 1 & 0 & 0 & 7 & 0 & 0 & 0 & 5 & 0 & 0 & 3 & 0 & 0 & 0 & 7 \\
& = & & & & 7 & 0 & 0 & 5 & 0 & 0 & 0 & 0 & 11 & 0 & 0 & 0 & 7 \\
& = & 1 & 0 & 0 & 0 & \overline{1} & 0 & 0 & 0 & 0 & 11 & 0 & 0 & 0 & 0 & 0 & \overline{9}
\end{array}
$$

N. Méloni
IMATH - Université de Toulon

Integer recoding in a nutshell

Let $k = 31415$

$\mathcal{D} = \{1, 2, 3, 4, 5, 6, 7\}$

$$
\begin{array}{rcccccccccccccccc}
k & = & & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\
& = & & & & 7 & 0 & 0 & 5 & 0 & 0 & 2 & 0 & 0 & 6 & 0 & 0 & 7 \\
& = & & 1 & 0 & 0 & 7 & 0 & 0 & 0 & 5 & 0 & 0 & 3 & 0 & 0 & 0 & 7 \\
& = & & & & 7 & 0 & 0 & 5 & 0 & 0 & 0 & 0 & 11 & 0 & 0 & 0 & 7 \\
& = & 1 & 0 & 0 & 0 & \overline{1} & 0 & 0 & 0 & 0 & 11 & 0 & 0 & 0 & 0 & 0 & \overline{9}
\end{array}
$$

N. Méloni
IMATH - Université de Toulon

Integer recoding in a nutshell

Let $k = 31415$

$\mathcal{D} = \{1, 2, 3, 4, 5, 6, 7\}$

$$
\begin{array}{rcccccccccccccccc}
k & = & & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\
 & = & & & & 7 & 0 & 0 & 5 & 0 & 0 & 2 & 0 & 0 & 6 & 0 & 0 & 7 \\
 & = & & 1 & 0 & 0 & 7 & 0 & 0 & 0 & 5 & 0 & 0 & 3 & 0 & 0 & 0 & 7 \\
 & = & & & & 7 & 0 & 0 & 5 & 0 & 0 & 0 & 0 & 11 & 0 & 0 & 0 & 7 \\
 & = & 1 & 0 & 0 & 0 & \overline{1} & 0 & 0 & 0 & 0 & 11 & 0 & 0 & 0 & 0 & 0 & \overline{9}
\end{array}
$$

N. Méloni
IMATH - Université de Toulon

Integer recoding in a nutshell

Let $k = 31415$

$\mathcal{D} = \{1, 3, 5, 7\}$

$$
\begin{array}{rcccccccccccccccc}
k & = & & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\
 & = & & & & 7 & 0 & 0 & 5 & 0 & 0 & 2 & 0 & 0 & 6 & 0 & 0 & 7 \\
 & = & & 1 & 0 & 0 & 7 & 0 & 0 & 0 & 5 & 0 & 0 & 3 & 0 & 0 & 0 & 7 \\
 & = & & & & 7 & 0 & 0 & 5 & 0 & 0 & 0 & 0 & 11 & 0 & 0 & 0 & 7 \\
 & = & 1 & 0 & 0 & 0 & \overline{1} & 0 & 0 & 0 & 0 & 11 & 0 & 0 & 0 & 0 & 0 & \overline{9}
\end{array}
$$

N. Méloni
IMATH - Université de Toulon

Integer recoding in a nutshell

Let $k = 31415$

$\mathcal{D} = \{1, 3, 5, 7\}$

$$
\begin{array}{rcccccccccccccccc}
k & = & & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\
 & = & & & & 7 & 0 & 0 & 5 & 0 & 0 & 2 & 0 & 0 & 6 & 0 & 0 & 7 \\
 & = & & 1 & 0 & 0 & 7 & 0 & 0 & 0 & 5 & 0 & 0 & 3 & 0 & 0 & 0 & 7 \\
 & = & & & & 7 & 0 & 0 & 5 & 0 & 0 & 0 & 0 & 11 & 0 & 0 & 0 & 7 \\
 & = & 1 & 0 & 0 & 0 & \overline{1} & 0 & 0 & 0 & 0 & 11 & 0 & 0 & 0 & 0 & 0 & \overline{9}
\end{array}
$$

N. Méloni
IMATH - Université de Toulon

Integer recoding in a nutshell

Let $k = 31415$

$\mathcal{D} = \{1, 3, 5, 7\}$

$$
\begin{array}{rcccccccccccccccc}
k & = & & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\
 & = & & & & 7 & 0 & 0 & 5 & 0 & 0 & 2 & 0 & 0 & 6 & 0 & 0 & 7 \\
 & = & & 1 & 0 & 0 & 7 & 0 & 0 & 0 & 5 & 0 & 0 & 3 & 0 & 0 & 0 & 7 \\
 & = & & & & 7 & 0 & 0 & 5 & 0 & 0 & 0 & 0 & 11 & 0 & 0 & 0 & 7 \\
 & = & 1 & 0 & 0 & 0 & \overline{1} & 0 & 0 & 0 & 0 & 11 & 0 & 0 & 0 & 0 & 0 & \overline{9}
\end{array}
$$

N. Méloni
IMATH - Université de Toulon

Integer recoding in a nutshell

Let $k = 31415$

$\mathcal{D} = \{1, 3, 5, 7\}$

$$
\begin{array}{rcccccccccccccccc}
k & = & & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\
 & = & & & & 7 & 0 & 0 & 5 & 0 & 0 & 2 & 0 & 0 & 6 & 0 & 0 & 7 \\
 & = & & 1 & 0 & 0 & 7 & 0 & 0 & 0 & 5 & 0 & 0 & 3 & 0 & 0 & 0 & 7 \\
 & = & & & & 7 & 0 & 0 & 5 & 0 & 0 & 0 & 0 & 11 & 0 & 0 & 0 & 7 \\
 & = & 1 & 0 & 0 & 0 & \overline{1} & 0 & 0 & 0 & 0 & 11 & 0 & 0 & 0 & 0 & 0 & \overline{9}
\end{array}
$$

N. Méloni
IMATH - Université de Toulon

Integer recoding in a nutshell

Let $k = 31415$

$\mathcal{D} = \{1, 3, 5, 7\}$

$$
\begin{array}{rcccccccccccccccc}
k & = & & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\
 & = & & & & 7 & 0 & 0 & 5 & 0 & 0 & 2 & 0 & 0 & 6 & 0 & 0 & 7 \\
 & = & & 1 & 0 & 0 & 7 & 0 & 0 & 0 & 5 & 0 & 0 & 3 & 0 & 0 & 0 & 7 \\
 & = & & & & 7 & 0 & 0 & 5 & 0 & 0 & 0 & 0 & 11 & 0 & 0 & 0 & 7 \\
 & = & 1 & 0 & 0 & 0 & \overline{1} & 0 & 0 & 0 & 0 & 11 & 0 & 0 & 0 & 0 & 0 & \overline{9}
\end{array}
$$

N. Méloni
IMATH - Université de Toulon

Integer recoding in a nutshell

Let $k = 31415$

$\mathcal{D} = \{1, 3, 5, 7\}$

$$
\begin{array}{rcccccccccccccccc}
k & = & & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\
 & = & & & & 7 & 0 & 0 & 5 & 0 & 0 & 2 & 0 & 0 & 6 & 0 & 0 & 7 \\
 & = & & 1 & 0 & 0 & 7 & 0 & 0 & 0 & 5 & 0 & 0 & 3 & 0 & 0 & 0 & 7 \\
 & = & & & & 7 & 0 & 0 & 5 & 0 & 0 & 0 & 0 & 11 & 0 & 0 & 0 & 7 \\
 & = & 1 & 0 & 0 & 0 & \overline{1} & 0 & 0 & 0 & 0 & 11 & 0 & 0 & 0 & 0 & 0 & \overline{9}
\end{array}
$$

N. Méloni
IMATH - Université de Toulon

Integer recoding in a nutshell

Let $k = 31415$

$\mathcal{D} = \{1, 3, 5, 7, 9, 11\}$

$$
\begin{array}{rcccccccccccccccc}
k & = & & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\
 & = & & & & 7 & 0 & 0 & 5 & 0 & 0 & 2 & 0 & 0 & 6 & 0 & 0 & 7 \\
 & = & & 1 & 0 & 0 & 7 & 0 & 0 & 0 & 5 & 0 & 0 & 3 & 0 & 0 & 0 & 7 \\
 & = & & & & 7 & 0 & 0 & 5 & 0 & 0 & 0 & 0 & 11 & 0 & 0 & 0 & 7 \\
 & = & 1 & 0 & 0 & 0 & \overline{1} & 0 & 0 & 0 & 0 & 11 & 0 & 0 & 0 & 0 & 0 & \overline{9}
\end{array}
$$

N. Méloni
IMATH - Université de Toulon

Integer recoding in a nutshell

Let $k = 31415$

$\mathcal{D} = \{1, 3, 5, 7, 9, 11\}$

$$
\begin{array}{rcccccccccccccccc}
k & = & & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\
 & = & & & & 7 & 0 & 0 & 5 & 0 & 0 & 2 & 0 & 0 & 6 & 0 & 0 & 7 \\
 & = & & 1 & 0 & 0 & 7 & 0 & 0 & 0 & 5 & 0 & 0 & 3 & 0 & 0 & 0 & 7 \\
 & = & & & & 7 & 0 & 0 & 5 & 0 & 0 & 0 & 0 & 11 & 0 & 0 & 0 & 7 \\
 & = & 1 & 0 & 0 & 0 & \overline{1} & 0 & 0 & 0 & 0 & 11 & 0 & 0 & 0 & 0 & 0 & \overline{9}
\end{array}
$$

N. Méloni
IMATH - Université de Toulon

Integer recoding in a nutshell

Let $k = 31415$

$\mathcal{D} = \{1, 3, 5, 7, 9, 11\}$

$$
\begin{array}{rcccccccccccccccc}
k & = & & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\
 & = & & & & 7 & 0 & 0 & 5 & 0 & 0 & 2 & 0 & 0 & 6 & 0 & 0 & 7 \\
 & = & & 1 & 0 & 0 & 7 & 0 & 0 & 0 & 5 & 0 & 0 & 3 & 0 & 0 & 0 & 7 \\
 & = & & & & 7 & 0 & 0 & 5 & 0 & 0 & 0 & 0 & 11 & 0 & 0 & 0 & 7 \\
 & = & 1 & 0 & 0 & 0 & \overline{1} & 0 & 0 & 0 & 0 & 11 & 0 & 0 & 0 & 0 & 0 & \overline{9}
\end{array}
$$

N. Méloni
IMATH - Université de Toulon

Integer recoding in a nutshell

Let $k = 31415$

$\mathcal{D} = \{1, 3, 5, 7, 9, 11\}$

$$
\begin{array}{rcccccccccccccccc}
k & = & & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\
 & = & & & & 7 & 0 & 0 & 5 & 0 & 0 & 2 & 0 & 0 & 6 & 0 & 0 & 7 \\
 & = & & 1 & 0 & 0 & 7 & 0 & 0 & 0 & 5 & 0 & 0 & 3 & 0 & 0 & 0 & 7 \\
 & = & & & & 7 & 0 & 0 & 5 & 0 & 0 & 0 & 0 & 11 & 0 & 0 & 0 & 7 \\
 & = & 1 & 0 & 0 & 0 & \overline{1} & 0 & 0 & 0 & 0 & 11 & 0 & 0 & 0 & 0 & 0 & \overline{9}
\end{array}
$$

N. Méloni
IMATH - Université de Toulon

Integer recoding in a nutshell

Let $k = 31415$

$\mathcal{D} = \{1, 3, 5, 7, 9, 11\}$

$$
\begin{array}{rcccccccccccccccc}
k & = & & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\
 & = & & & & 7 & 0 & 0 & 5 & 0 & 0 & 2 & 0 & 0 & 6 & 0 & 0 & 7 \\
 & = & & 1 & 0 & 0 & 7 & 0 & 0 & 0 & 5 & 0 & 0 & 3 & 0 & 0 & 0 & 7 \\
 & = & & & & 7 & 0 & 0 & 5 & 0 & 0 & 0 & 0 & 11 & 0 & 0 & 0 & 7 \\
 & = & 1 & 0 & 0 & 0 & \overline{1} & 0 & 0 & 0 & 0 & 11 & 0 & 0 & 0 & 0 & 0 & \overline{9}
\end{array}
$$

N. Méloni
IMATH - Université de Toulon

Integer recoding in a nutshell

Let $k = 31415$

$\mathcal{D} = \{1, 3, 5, 7, 9, 11\}$

$$
\begin{array}{rcccccccccccccccc}
k & = & & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\
 & = & & & & 7 & 0 & 0 & 5 & 0 & 0 & 2 & 0 & 0 & 6 & 0 & 0 & 7 \\
 & = & & 1 & 0 & 0 & 7 & 0 & 0 & 0 & 5 & 0 & 0 & 3 & 0 & 0 & 0 & 7 \\
 & = & & & & 7 & 0 & 0 & 5 & 0 & 0 & 0 & 0 & 11 & 0 & 0 & 0 & 7 \\
 & = & 1 & 0 & 0 & 0 & \overline{1} & 0 & 0 & 0 & 0 & 11 & 0 & 0 & 0 & 0 & 0 & \overline{9}
\end{array}
$$

N. Méloni
IMATH - Université de Toulon

Integer recoding in a nutshell

Let $k = 31415$

$\mathcal{D} = \{1, 3, 5, 7, 9, 11\}$

$$
\begin{array}{rcccccccccccccccc}
k & = & & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & & 1 & 1 & & 0 & 1 & 1 & 1 \\
 & = & & & & 7 & 0 & 0 & 5 & 0 & 0 & 2 & & 0 & 0 & & 6 & 0 & 0 & 7 \\
 & = & & 1 & 0 & 0 & 7 & 0 & 0 & 0 & 5 & 0 & & 0 & 3 & & 0 & 0 & 0 & 7 \\
 & = & & & & & 7 & 0 & 0 & 5 & 0 & 0 & & 0 & 11 & & 0 & 0 & 0 & 7 \\
 & = & 1 & 0 & 0 & 0 & \overline{1} & 0 & 0 & 0 & 0 & 11 & & 0 & 0 & & 0 & 0 & 0 & \overline{9}
\end{array}
$$

N. Méloni
IMATH - Université de Toulon

Integer recoding in a nutshell

Let $k = 31415$

$\mathcal{D} = \{1, 3, 5, 7, 9, 11\}$

$$
\begin{array}{rcccccccccccccccc}
k & = & & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\
 & = & & & & 7 & 0 & 0 & 5 & 0 & 0 & 2 & 0 & 0 & 6 & 0 & 0 & 7 \\
 & = & & 1 & 0 & 0 & 7 & 0 & 0 & 0 & 5 & 0 & 0 & 3 & 0 & 0 & 0 & 7 \\
 & = & & & & 7 & 0 & 0 & 5 & 0 & 0 & 0 & 0 & 11 & 0 & 0 & 0 & 7 \\
 & = & 1 & 0 & 0 & 0 & \overline{1} & 0 & 0 & 0 & 0 & 11 & 0 & 0 & 0 & 0 & 0 & \overline{9}
\end{array}
$$

N. Méloni
IMATH - Université de Toulon

Integer recoding in a nutshell

Let $k = 31415$

$\mathcal{D} = \{1, 3, 5, 7, 9, 11\}$

$$
\begin{array}{rcccccccccccccccc}
k & = & & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\
 & = & & & & 7 & 0 & 0 & 5 & 0 & 0 & 2 & 0 & 0 & 6 & 0 & 0 & 7 \\
 & = & & 1 & 0 & 0 & 7 & 0 & 0 & 0 & 5 & 0 & 0 & 3 & 0 & 0 & 0 & 7 \\
 & = & & & & 7 & 0 & 0 & 5 & 0 & 0 & 0 & 0 & 11 & 0 & 0 & 0 & 7 \\
 & = & 1 & 0 & 0 & 0 & \overline{1} & 0 & 0 & 0 & 0 & 11 & 0 & 0 & 0 & 0 & 0 & \overline{9}
\end{array}
$$

N. Méloni
IMATH - Université de Toulon

Integer recoding in a nutshell

Let $k = 31415$

$\mathcal{D} = \{1, 3, 5, 7, 9, 11\}$

$$
\begin{array}{rcccccccccccccccc}
k & = & & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\
 & = & & & & 7 & 0 & 0 & 5 & 0 & 0 & 2 & 0 & 0 & 6 & 0 & 0 & 7 \\
 & = & & 1 & 0 & 0 & 7 & 0 & 0 & 0 & 5 & 0 & 0 & 3 & 0 & 0 & 0 & 7 \\
 & = & & & & 7 & 0 & 0 & 5 & 0 & 0 & 0 & 0 & 11 & 0 & 0 & 0 & 7 \\
 & = & 1 & 0 & 0 & 0 & \overline{1} & 0 & 0 & 0 & 0 & 11 & 0 & 0 & 0 & 0 & 0 & \overline{9}
\end{array}
$$

N. Méloni
IMATH - Université de Toulon

Integer recoding in a nutshell

Let $k = 31415$

$\mathcal{D} = \{\pm 1, \pm 3, \pm 5, \pm 7, \pm 9, \pm 11\}$

$$
\begin{array}{rcccccccccccccccc}
k & = & & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\
 & = & & & & 7 & 0 & 0 & 5 & 0 & 0 & 2 & 0 & 0 & 6 & 0 & 0 & 7 \\
 & = & & 1 & 0 & 0 & 7 & 0 & 0 & 0 & 5 & 0 & 0 & 3 & 0 & 0 & 0 & 7 \\
 & = & & & & 7 & 0 & 0 & 5 & 0 & 0 & 0 & 0 & 11 & 0 & 0 & 0 & 7 \\
 & = & 1 & 0 & 0 & 0 & \overline{1} & 0 & 0 & 0 & 0 & 11 & 0 & 0 & 0 & 0 & 0 & \overline{9}
\end{array}
$$

N. Méloni
IMATH - Université de Toulon

Integer recoding in a nutshell

Let $k = 31415$

$\mathcal{D} = \{\pm 1, \pm 3, \pm 5, \pm 7, \pm 9, \pm 11\}$

$$
\begin{array}{rcccccccccccccccc}
k & = & & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\
 & = & & & & 7 & 0 & 0 & 5 & 0 & 0 & 2 & 0 & 0 & 6 & 0 & 0 & 7 \\
 & = & & 1 & 0 & 0 & 7 & 0 & 0 & 0 & 5 & 0 & 0 & 3 & 0 & 0 & 0 & 7 \\
 & = & & & & 7 & 0 & 0 & 5 & 0 & 0 & 0 & 0 & 11 & 0 & 0 & 0 & 7 \\
 & = & 1 & 0 & 0 & 0 & \overline{1} & 0 & 0 & 0 & 0 & 11 & 0 & 0 & 0 & 0 & 0 & \overline{9}
\end{array}
$$

N. Méloni
IMATH - Université de Toulon

frac-w-NAF properties

- $\mathcal{D} = \{\pm 1, \pm 3, \pm 5, \ldots, \pm(2n-1)\}$
- density: $\frac{1}{a+1}$, where

$$a = W_n + \frac{2n}{2^{W_n}}$$

and

$$W_n = \lfloor \log_2(2n-1) \rfloor$$

- example: $\mathcal{D} = \{\pm 1, \pm 3, \pm 5, \pm 7\}$ then $a = 2 + 8/4 = 4$.

N. Méloni
IMATH - Université de Toulon

$\mathcal{D}$-representation

Definition

- $\mathcal{D} = \{d_1, \ldots, d_n\} \subset \mathbb{N}$
- $\bar{\mathcal{D}} = \mathcal{D} \cup \{-d_1, \ldots, -d_n\}$
- k an integer
-

$$k = \sum_{i=0}^{l-1} k_i 2^i = (k_{l-1} \ldots k_1 k_0)_2$$

$$k_i \in \bar{\mathcal{D}} \cup \{0\}$$

N. Méloni
IMATH - Université de Toulon

$\mathcal{D}$-representation

Examples

- $\mathcal{D} = \{1\} \rightarrow$ NAF

$$\begin{aligned} 31415 &= 2^{15} - 2^{10} - 2^8 - 2^6 - 2^3 - 1 \\ &= (1000\bar{1}0\bar{1}0\bar{1}00\bar{1}00\bar{1})_2 \end{aligned}$$

- $\mathcal{D} = \{1, 3, 5, 7\} \rightarrow$ 4-NAF

$$\begin{aligned} 31415 &= 2^{15} - 5 \cdot 2^8 - 5 \cdot 2^4 + 7 \\ &= (1000000\bar{5}000\bar{5}0007)_2 \end{aligned}$$

N. Méloni
IMATH - Université de Toulon

Existence

Let $N(\mathcal{D}) = \{\sum_{i=0}^{l-1} k_i 2^i : k_i \in \overline{\mathcal{D}}\}$.

- $k \in N(\mathcal{D}) \Rightarrow \gcd(\{d_1, \ldots, d_n\})|k$

We want $N(\mathcal{D}) = \mathbb{Z}$.

- Necessary condition: $\gcd(\{d_1, \ldots, d_n\}) = 1$
- Sufficient condition: $1 \in \mathcal{D}$

We fix $d_1 = 1$.

Construction

$\mathcal{D} = \{1, 7, 13\}$

k	=	1	1	1	1	0	1	0	1	0	1	1	0	1	1	1
1	=															1
7	=													1	1	1
13	=												1	1	0	1

Construction

$\mathcal{D} = \{1, 7, 13\}$

k	=	1	1	1	1	0	1	0	1	0	1	1	0	1	1	1
1	=															1
7	=													1	1	1
13	=												1	1	0	1

N. Méloni
IMATH - Université de Toulon

Construction

$\mathcal{D} = \{1, 7, 13\}$

k	$=$	1	1	1	1	0	1	0	1	0	1	1	0	1	1	1
1	$=$															1
7	$=$													1	1	1
13	$=$												1	1	0	1

N. Méloni
IMATH - Université de Toulon

Construction

$\mathcal{D} = \{1, 7, 13\}$

k	=	1	1	1	1	0	1	0	1	0	1	1	0	0	0	7
1	=															1
7	=													1	1	1
13	=												1	1	0	1

Construction

$\mathcal{D} = \{1, 7, 13\}$

k	=	1	1	1	1	0	1	0	1	0	1	1	0	0	0	7
1	=															1
7	=													1	1	1
13	=												1	1	0	1

N. Méloni
IMATH - Université de Toulon

Construction

$\mathcal{D} = \{1, 7, 13\}$

k	=	1	1	1	1	0	1	0	1	0	1	1	0	0	0	7
1	=															1
7	=													1	1	1
13	=												1	1	0	1

Construction

$\mathcal{D} = \{1, 7, 13\}$

k	$=$	1	1	1	1	0	1	0	1	0	1	1	0	0	0	7
1	$=$															1
7	$=$													1	1	1
13	$=$												1	1	0	1

N. Méloni
IMATH - Université de Toulon

Construction

$\mathcal{D} = \{1, 7, 13\}$

k	=	1	1	1	1	0	1	0	1	0	1	1	0	0	0	7
1	=															1
7	=													1	1	1
13	=												1	1	0	1

	1	1	1	1	0	1	0	1	0	1	1
-									1	1	1
=	1	1	1	1	0	1	0	0	1	0	0

N. Méloni
IMATH - Université de Toulon

Construction

$\mathcal{D} = \{1, 7, 13\}$

k	=	1	1	1	1	0	1	0	0	1	0	7	0	0	0	7
1	=															1
7	=													1	1	1
13	=												1	1	0	1

	1	1	1	1	0	1	0	1	0	1	1
-									1	1	1
=	1	1	1	1	0	1	0	0	1	0	0

N. Méloni
IMATH - Université de Toulon

Construction

$\mathcal{D} = \{1, 7, 13\}$

k	=	1	1	1	1	0	1	0	0	1	0	7	0	0	0	7
1	=															1
7	=													1	1	1
13	=												1	1	0	1

Construction

$\mathcal{D} = \{1, 7, 13\}$

k	=	1	1	1	1	0	1	0	0	1	0	7	0	0	0	7
1	=															1
7	=													1	1	1
13	=												1	1	0	1

Construction

$\mathcal{D} = \{1, 7, 13\}$

k	$=$	1	1	1	1	0	1	0	0	1	0	7	0	0	0	7
1	$=$															1
7	$=$													1	1	1
13	$=$												1	1	0	1

N. Méloni
IMATH - Université de Toulon

Construction

$\mathcal{D} = \{1, 7, 13\}$

k	=	1	1	1	1	0	1	0	0	1	0	7	0	0	0	7
1	=															1
7	=													1	1	1
13	=												1	1	0	1

Construction

$\mathcal{D} = \{1, 7, 13\}$

k	=	1	1	1	1	0	1	0	0	1	0	7	0	0	0	7
1	=															1
7	=													1	1	1
13	=												1	1	0	1

Construction

$\mathcal{D} = \{1, 7, 13\}$

k	$=$	1	1	1	1	0	1	0	0	1	0	7	0	0	0	7
1	$=$															1
7	$=$													1	1	1
13	$=$												1	1	0	1

Construction

$\mathcal{D} = \{1, 7, 13\}$

k	=	1	1	0	0	0	13	0	0	1	0	7	0	0	0	7
1	=															1
7	=													1	1	1
13	=												1	1	0	1

Construction

$\mathcal{D} = \{1, 7, 13\}$

k	=	1	1	0	0	0	13	0	0	1	0	7	0	0	0	7
1	=															1
7	=													1	1	1
13	=												1	1	0	1

Construction

$\mathcal{D} = \{1, 7, 13\}$

k	=	1	1	0	0	0	13	0	0	1	0	7	0	0	0	7
1	=															1
7	=													1	1	1
13	=												1	1	0	1

Construction

$\mathcal{D} = \{1, 7, 13\}$

k	=	1	1	0	0	0	13	0	0	1	0	7	0	0	0	7
1	=															1
7	=													1	1	1
13	=												1	1	0	1

N. Méloni
IMATH - Université de Toulon

Construction

$\mathcal{D} = \{1, 7, 13\}$

k	=	1	1	0	0	0	13	0	0	1	0	7	0	0	0	7
1	=															1
7	=													1	1	1
13	=												1	1	0	1

Construction

$\mathcal{D} = \{1, 7, 13\}$

k	=	1	1	0	0	0	13	0	0	1	0	7	0	0	0	7
1	=															1
7	=													1	1	1
13	=												1	1	0	1

Construction

$\mathcal{D} = \{1, 7, 13\}$

k	=	1	1	0	0	0	13	0	0	1	0	7	0	0	0	7
1	=															1
7	=													1	1	1
13	=												1	1	0	1

Residue sets

Let $\mathcal{D} = \{1, d_2, \ldots, d_n\}$. Let w such that $1 \leq w \leq \log_2(\max(d_i)) + 1$, $\mathcal{D}_w = \{d_i \mod 2^w, i = 1 \ldots n\}$, $\overline{\mathcal{D}}_w = \mathcal{D}_w \cup \{-d_i \mod 2^w\}$.

Example

$$
\begin{array}{lcllcl}
\mathcal{D} & = & \{1, 7, 13\} & & & \\
\mathcal{D}_1 & = & \{1\} & \overline{\mathcal{D}}_1 & = & \{1\} \\
\mathcal{D}_2 & = & \{1, 3\} & \overline{\mathcal{D}}_2 & = & \{1, 3\} \\
\mathcal{D}_3 & = & \{1, 5, 7\} & \overline{\mathcal{D}}_3 & = & \{1, 3, 5, 7\} \\
\mathcal{D}_4 & = & \{1, 7, 13\} & \overline{\mathcal{D}}_4 & = & \{1, 3, 7, 9, 13, 15\}
\end{array}
$$

N. Méloni
IMATH - Université de Toulon

Recoding algortihm

Require: An integer k and a set $\mathcal{D} = \{1, d_2, \ldots, d_n\}$
Ensure: $k = (k_t k_{t-1} \ldots k_1 k_0)_2$, $k_i \in \overline{\mathcal{D}} \cup \{0\}$

1: $i = 0$
2: **while** $k \neq 0$ **do**
3: $\quad k_i = digit_{\mathcal{D}}(k)$
4: $\quad k = \frac{k - k_i}{2}$
5: $\quad i = i + 1$
6: **end while**
7: **return** $(k_{i-1} \ldots k_0)$

N. Méloni
IMATH - Université de Toulon

Average Density

Theorem

Let

- $\mathcal{D} = \{1, d_2, \ldots, d_n\}$,
- $W_n = \lfloor \log_2(\max(d_i)) \rfloor$,
- $D(w) = \frac{\#\overline{\mathcal{D}}_w}{2^{w-1}}$.

The average number of non-zero digits is $\frac{1}{a_{\mathcal{D}}+1}$, where

$$a_{\mathcal{D}} = 2D(W_n + 2) + \sum_{w=2}^{W_n+1} D(w).$$

N. Méloni
IMATH - Université de Toulon

Applications

- $\mathcal{D} = \{1, 3, \ldots, 2n-1\}$
  - $W_n = \lfloor \log_2(2n-1) \rfloor$,
  - $D(W_n + 1) = D(W_n) = \cdots = D(2) = 1$,
  - $a_{\mathcal{D}} = W_n + \frac{2n}{2^{W_n}}$.
- $\mathcal{D} = \{1, 3, 23, 27\}$
  - $\overline{\mathcal{D}}_2 = \{1, 3\}$, $\overline{\mathcal{D}}_3 = \{1, 3, 5, 7\}$, $\overline{\mathcal{D}}_4 = \{1, 3, 5, 7, 9, 11, 13, 15\}$, $\overline{\mathcal{D}}_5 = \{1, 3, 5, 9, 23, 27, 29, 31\}$
  - $a_{\mathcal{D}} = 2 \times \frac{1}{4} + \frac{1}{2} + 1 + 1 + 1 = 4$.
  - Same density as 4-NAF where $\mathcal{D} = \{1, 3, 5, 7\}$.

Optimal digit sets

Definition

Let $n > 0$ and $\mathbb{D}_n$ be the set of all sets of odd integers of the form $\{1, d_2, \ldots, d_n\}$. Then $\mathcal{D} \in \mathbb{D}_n$ is an **optimal digit set** if

$$a_{\mathcal{D}} = \max_{\mathcal{D}' \in \mathbb{D}_n} (a_{\mathcal{D}'}).$$

Theorem

Let $w_n = \lfloor \log_2 n \rfloor$. $\mathcal{D}$ is optimal if and only if

$$a_{\mathcal{D}} = w_n + \frac{n}{2^{w_n}} + 1.$$

N. Méloni
IMATH - Université de Toulon

Optimal digit sets

Corollary 1

$\mathcal{D}$ is an optimal digit set if and only if:

$$\#\overline{\mathcal{D}}_{w_n+3} = 2n \text{ and } \#\overline{\mathcal{D}}_{w_n+2} = 2^{w_n+1}.$$

Corollary 2

For any $n > 0$, there are infinitely many optimal digit sets of cardinal n.

N. Méloni
IMATH - Université de Toulon

Randomize representations

Randomize scheme

- Set m and l such that $l \leq (m+1)/2$
- For any integer k, pick $l-1$ integers $\{d_2, \ldots, d_l\}$ among $\{3, \ldots, m\}$
- Compute the $\mathcal{D}$-representation of k.

- What is the average density of non-zero terms?

N. Méloni
IMATH - Université de Toulon

Evaluating $D(w)$

- To apply the theorem we need to know the value of $D(w)$ and thus, that of $\#\mathcal{D}_w$
- Consists of counting the average number of classes modulo 2^w given a random set $\mathcal{D}$.

Example: $w = 3$, there are 4 classes: 1,3,5,7

$\mathcal{D} \quad = \{d_1, d_2, d_3, d_4, d_5, d_6, d_7, d_8, d_9\}$

Draw l integers, how many classes on average?

Evaluating $D(w)$

- To apply the theorem we need to know the value of $D(w)$ and thus, that of $\#\mathcal{D}_w$
- Consists of counting the average number of classes modulo 2^w given a random set $\mathcal{D}$.

Example: $w = 3$, there are 4 classes: 1,3,5,7

$\mathcal{D} = \{d_1, d_2, d_3, d_4, d_5, d_6, d_7, d_8, d_9\}$

Draw l integers, how many classes on average?

Urn problem

$M(l, c, N)$: number of draws of l balls among N of c different colors. Probability of having 4 colors:

$$P[X = 4] = \frac{M(5, 4, 9)}{\binom{9}{5}}$$

Urn problem

$M(l, c, N)$: number of draws of l balls among N of c different colors. Probability of having 4 colors:

$$P[X = 4] = \frac{M(5, 4, 9)}{\binom{9}{5}}$$

M depends on the number of representative of each class.

Walton's Theorem

Theorem (Walton 86)

Let E_w^i be the number of representatives of class i modulo 2^w.

$$\prod_{c=1}^{C_w} \left(Y\{(1+X)^{E_w^i} - 1\} + 1 \right) = \sum_c \sum_l M(l, c, N) X^l Y^c$$

N. Méloni
IMATH - Université de Toulon

Walton's Theorem

- $w = 3$, we have 4 classes: 1,3,5,7
  $\mathcal{D} = \{d_1, d_2, d_3, d_4, d_5, d_6, d_7, d_8, d_9\}$
- $(Y((1+X)^3-1)+1)(Y((1+X)^2-1)+1)^3 =$
  $(X^9+9X^8+33X^7+62X^6+60X^5+24X^4)Y^4$
  $+(3X^7+22X^6+63X^5+84X^4+44X^3)Y^3$
  $+(3X^5+18X^4+39X^3+30X^2)Y^2$
  $+(X^3+6X^2+9X)Y+1$
- $P[X=4] = \frac{M(5,4,9)}{\binom{9}{5}} = \frac{60}{126} = \frac{10}{21}$

N. Méloni
IMATH - Université de Toulon

Walton's Theorem

- $w = 3$, we have 4 classes: 1,3,5,7
  $\mathcal{D} = \{d_1, d_2, d_3, d_4, d_5, d_6, d_7, d_8, d_9\}$
- $(Y((1+X)^3-1)+1)(Y((1+X)^2-1)+1)^3 =$
  $(X^9+9X^8+33X^7+62X^6+60X^5+24X^4)Y^4$
  $+(3X^7+22X^6+63X^5+84X^4+44X^3)Y^3$
  $+(3X^5+18X^4+39X^3+30X^2)Y^2$
  $+(X^3+6X^2+9X)Y+1$
- $P[X=4] = \frac{M(5,4,9)}{\binom{9}{5}} = \frac{60}{126} = \frac{10}{21}$

N. Méloni
IMATH - Université de Toulon

Walton's Theorem

- $w = 3$, we have 4 classes: 1,3,5,7
  $\mathcal{D} = \{d_1, d_2, d_3, d_4, d_5, d_6, d_7, d_8, d_9\}$
- $(Y((1+X)^3-1)+1)(Y((1+X)^2-1)+1)^3 =$
  $(X^9+9X^8+33X^7+62X^6+60X^5+24X^4)Y^4$
  $+(3X^7+22X^6+63X^5+84X^4+44X^3)Y^3$
  $+(3X^5+18X^4+39X^3+30X^2)Y^2$
  $+(X^3+6X^2+9X)Y+1$
- $P[X=4] = \frac{M(5,4,9)}{\binom{9}{5}} = \frac{60}{126} = \frac{10}{21}$

Walton's Theorem

- $w = 3$, we have 4 classes: 1,3,5,7
  $\mathcal{D} = \{d_1, d_2, d_3, d_4, d_5, d_6, d_7, d_8, d_9\}$
- $(Y((1+X)^3-1)+1)(Y((1+X)^2-1)+1)^3 =$
  $(X^9+9X^8+33X^7+62X^6+60X^5+24X^4)Y^4$
  $+(3X^7+22X^6+63X^5+84X^4+44X^3)Y^3$
  $+(3X^5+18X^4+39X^3+30X^2)Y^2$
  $+(X^3+6X^2+9X)Y+1$
- $P[X=4] = \frac{M(5,4,9)}{\binom{9}{5}} = \frac{60}{126} = \frac{10}{21}$

N. Méloni
IMATH - Université de Toulon

Some numbers

m	$\#\mathcal{D}$	RDR	wNAF
7	2	3.833	4
15	4	4.771	5
31	8	5.728	6
63	16	6.706	7
127	32	7.695	8
255	64	8.689	9
511	128	9.686	10
1023	256	10.69	11

Inverses of the density of the RDR and wNAF using $\left\lfloor \frac{m+1}{4} \right\rfloor$ digits

N. Méloni
IMATH - Université de Toulon

Digit set size	Method	$a_{\mathcal{D}}+1$	group operation count
8	RDR	5.701	1023S+191M
	Opt. RDR	5.970	1024S+183M
	frac-wNAF	5.997	1023S+178M
16	RDR	6.666	1023S+175M
	Opt. RDR	6.960	1023S+169M
	frac-wNAF	6.962	1022S+161M
24	RDR	7.209	1023S+175M
	Opt. RDR	7.454	1023S+167M
	frac-wNAF	7.454	1023S+160M
32	RDR	7.634	1023S+175M
	Opt. RDR	7.940	1023S+170M
	frac-wNAF	7.950	1022S+160M
64	RDR	8.692	1023S+207M
	Opt. RDR	8.922	1023S+196M
	frac-wNAF	8.940	1022S+177M

Conclusions

- Exponentiation performs well with random digits
- Some important parts are missing!
  - How to compute $\{g^{d_i} : 1 \leq i \leq n\}$?
  - How does $digit_{\mathcal{D}}$ actally work?
- What is the point of all that?

Conclusions

- Exponentiation performs well with random digits
- Some important parts are missing!
  - How to compute $\{g^{d_i} : 1 \leq i \leq n\}$?
  - How does $digit_{\mathcal{D}}$ actally work?
- What is the point of all that?

Thank you for your attention.