

Cryptographic applications of weak restricted integer compositions

Gustavo Zambonin

Joint work with Lucas Perin, Ricardo Custódio, Lucia Moura and Daniel Panario.



uOttawa

University of Ottawa

`gustavo.zambonin@uottawa.ca`

June 6th, 2021

25th Ontario Combinatorics Workshop

Introduction

A partition of s is a representation of s as a sum

$$s = a_1 + a_2 + \cdots + a_t$$

with s, t positive, and each a_i with $1 \leq i \leq t$ is called a *part*.

The order of the parts *does not matter* for partitions. When it does, we are discussing *integer compositions*.

We present an application of integer compositions in cryptographic algorithms called signature schemes.

Examples of partitions and compositions

We list below all possible 16 compositions of $s = 5$.

<u>5</u> ,	$1 + 4$,
<u>$4 + 1$</u> ,	$1 + 3 + 1$,
<u>$3 + 2$</u> ,	$1 + 2 + 2$,
<u>$3 + 1 + 1$</u> ,	$1 + 2 + 1 + 1$,
$2 + 3$,	$1 + 1 + 3$,
<u>$2 + 2 + 1$</u> ,	$1 + 1 + 2 + 1$,
$2 + 1 + 2$,	$1 + 1 + 1 + 2$,
<u>$2 + 1 + 1 + 1$</u> ,	<u>$1 + 1 + 1 + 1 + 1$</u> .

Weak compositions

A composition where parts can be zero, of which there are infinitely many for any s .

We are interested in those with a limited number t of parts, denoted *weak t -compositions*.

Let $s = 7$ and $t = 5$. We can represent $4 + 0 + 1 + 2 + 0$ as shown below.

★ ★ ★ ★ | | ★ | ★ ★ |

In other words, we have a bijection to s stars and $t - 1$ bars. The number of weak t -compositions of s is $C(s, t) = \binom{s+t-1}{s}$.

Restricted compositions

Let S be a set of non-negative integers. An S -restricted composition is a composition of s such that all parts lie in S .

If $S = \{0, 1, \dots, n\}$ for n positive, we simply call the compositions n -restricted.

The number of n -restricted t -compositions of s is the coefficient of x^s in $(1 + x + x^2 + \dots + x^n)^t$, or equivalently

$$C(s, t, n) = \sum_{i=0}^{\min(t, \lfloor \frac{s}{n+1} \rfloor)} (-1)^i \binom{t}{i} \binom{s - (n+1)i + t - 1}{t-1}$$

as given by Eger [Ege13]. We note that $C(s, t) = C(s, t, s)$.

Examples of *weak* and restricted compositions

Let $s = 6$, $t = 3$ and $n = 3$. We list below all 28 weak compositions of 6 with 3 parts.

$$0 + 0 + 6$$

$$0 + 1 + 5$$

$$0 + 2 + 4$$

$$\underline{0 + 3 + 3}$$

$$0 + 4 + 2$$

$$0 + 5 + 1$$

$$0 + 6 + 0$$

$$1 + 0 + 5$$

$$1 + 1 + 4$$

$$\underline{1 + 2 + 3}$$

$$\underline{1 + 3 + 2}$$

$$1 + 4 + 1$$

$$1 + 5 + 0$$

$$2 + 0 + 4$$

$$\underline{2 + 1 + 3}$$

$$\underline{2 + 2 + 2}$$

$$\underline{2 + 3 + 1}$$

$$2 + 4 + 0$$

$$\underline{3 + 0 + 3}$$

$$\underline{3 + 1 + 2}$$

$$\underline{3 + 2 + 1}$$

$$\underline{3 + 3 + 0}$$

$$4 + 0 + 2$$

$$4 + 1 + 1$$

$$4 + 2 + 0$$

$$5 + 0 + 1$$

$$5 + 1 + 0$$

$$6 + 0 + 0$$

Ranking (combinatorial) objects

Let S be a finite set, $N = |S|$ and consider any distinct $s, t \in S$.

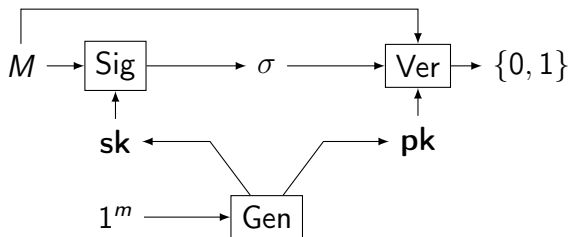
A *ranking function* is a bijection $\mathcal{R} : S \rightarrow \{0, \dots, N-1\}$ which defines a total ordering $\prec$ on the elements of S , i.e. $s \prec t \Leftrightarrow \mathcal{R}(s) \prec \mathcal{R}(t)$.

An *unranking function* is a bijection $\mathcal{U} : \{0, \dots, N-1\} \rightarrow S$ such that $\mathcal{R}(s) = i \Leftrightarrow \mathcal{U}(i) = s$ for all $0 \leq i \leq N-1$.

The total ordering is usually taken to be the lexicographic order $\prec_{\text{lex}}$.

Signature schemes

A mathematical framework that provides authentication, integrity and non-repudiation.



They are widely used in secure communications (HTTPS, package signing, digital certificates...) and thus need to be efficient. Some examples are RSA and elliptic-curve DSA.

Winternitz one-time signature scheme

A quantum-safe signature scheme used as a building block for many-time hash-based signatures.

We mainly discuss operations on signatures. A complete description is given by Hülsing *et al.* [HBG⁺18].

Let m be a positive integer called the security parameter. Let w be a positive integer that controls a performance trade-off.

Consider a message $0 \leq M \leq 2^m - 1$. To sign M , we initially divide it into a t -tuple of base- w integers, with $t = \lceil \frac{m}{\log_2 w} \rceil$.

Creating a Winternitz signature

Let $m = 32$, $w = 16$ and $M = 1\,996\,026\,778$. By converting M to binary, we have

$$\underbrace{\underbrace{0111}_{\log_2 w} \ 0110 \ 1111 \ 1000}_{m} \ 1111 \ 0011 \ 1001 \ 1010$$

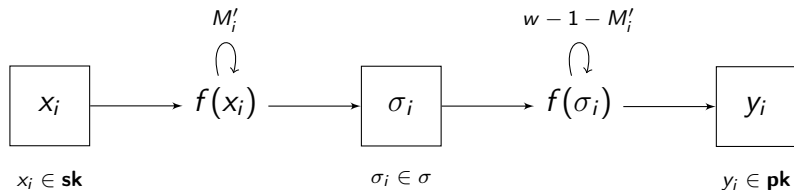
which is mapped to $M' = (7, 6, 15, 8, 15, 3, 9, 10)$.

In other words, we obtain a w -restricted t -composition of some integer $0 \leq k \leq t(w - 1)$.

This is a way of unranking M into t -tuples of base- w integers in $\prec_{\text{lex}}$.

Signing and verifying with Winternitz

Let f be a cryptographic hash function and $0 \leq i \leq t - 1$.



We note that $\mathbf{pk}$ is $\mathbf{sk}$ after w applications of f to each block.

The cost of operating on Winternitz signatures is *proportional* to the magnitude of M .

“Constant-sum” Winternitz [PZC⁺21]

It is useful if a cryptographic algorithm can be applied to distinct use cases, e.g. hardware tokens or document silos for long-term preservation.

We replace the Winternitz “base- w ” unranking with a bijection between messages and n -restricted t -compositions of s such that $C(s, t, n) \geq 2^m$.

Because M' will now always sum to s , we can predict the computational effort of creating signatures more accurately.

We provide several new unranking algorithms, practical experiments and a proof that our modification is secure.

The DCS algorithm [PZC⁺21, Alg. 1]

Input: $t, n, s \in \mathbb{N}$, $M \in \{0, \dots, 2^m - 1\}$, $y = (0, \dots, 0)$

Output: M' , the n -restricted t -composition of s in $\prec_{\text{lex}}$ corresponding to M

if $t = 1$ **then**

$M'_0 \leftarrow s$
 return M'

$b \leftarrow 0$

$\ell_l \leftarrow 0$

$\ell_r \leftarrow C(s, t - 1, n)$

while not $\ell_l \leq M < \ell_r$ **do**

$b \leftarrow b + 1$
 $\ell_l \leftarrow \ell_r$
 $\ell_r \leftarrow \ell_r + C(s - b, t - 1, n)$

$M'_{t-1} \leftarrow b$

DCS($t - 1, n, s - b, M - \ell_l, M'$)

return M'

Efficiency of “constant-sum” unranking

The “base- w ” unranking is extremely efficient, consisting only of bit manipulations.

However, the calculation of $C(*, *, n)$ in the main loop of **DCS** implies in several costly binomial computations.

The “constant-sum” unranking overhead becomes non-trivial when signing M . In our paper, we discuss solutions to this problem, including another algorithm called **DBCS**.

In this talk, we give preliminary results on a new algorithm based on **DCS**.

Rationale on the improved algorithm

Instead of calculating $C(s - b, t - 1, n)$, we store the partial values of $C(s, t - 1, n)$ and obtain smaller binomial coefficients via basic arithmetic operations.

For $0 \leq i \leq \min(t - 1, \lfloor \frac{s-b}{n+1} \rfloor)$ and $1 \leq b \leq s$, this ratio is

$$\frac{(-1)^i \binom{t-1}{i} \binom{(s-b)-(n+1)i+t-2}{t-2}}{(-1)^i \binom{t-1}{i} \binom{s-(n+1)i+t-2}{t-2}}.$$

Expanding the binomials gives us

$$\prod_{g=1}^b \frac{(s - g + 1) - (n + 1)i + t - 2}{(s - g + 1) - (n + 1)i},$$

which is a constant ratio for fixed g and i .

The improved DCS algorithm, DCS^+

Input: $t, n, s \in \mathbb{N}$, $M \in \{0, \dots, 2^m - 1\}$, $M' = (0, \dots, 0)$

Output: M' , the n -restricted t -composition of s in $\prec_{\text{lex}}$ corresponding to M

```

if  $t = 1$  then
     $M'_0 \leftarrow s$ 
    return  $M'$ 

 $b \leftarrow 0$ ;  $\ell_l \leftarrow 0$ ;  $\ell_r \leftarrow 0$ ;  $x \leftarrow [0, \dots, 0]$ 

for  $i \leftarrow 0$  to  $\min(t-1, \lfloor \frac{s}{n+1} \rfloor)$  do // terms of  $\ell_r$  are saved into  $x$ 
     $x_i \leftarrow (-1)^i \binom{t-1}{i} \binom{s-(n+1)i+t-2}{t-2}$ 
     $\ell_r \leftarrow \ell_r + x_i$ 

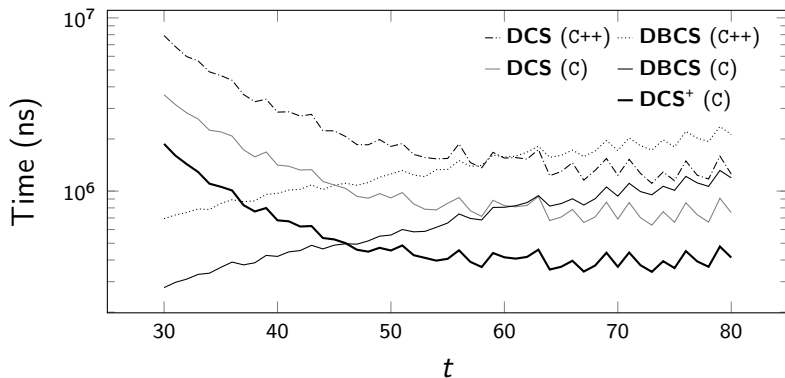
while  $M \geq \ell_r$  do
     $b \leftarrow b + 1$ 
     $\ell_l \leftarrow \ell_r$ 
     $u \leftarrow s - b + 1$ 
     $M \leftarrow (s - b + 1) + t - 2$ 
    for  $i \leftarrow 0$  to  $\min(t-1, \lfloor \frac{s-b}{n+1} \rfloor)$  do
        // compute each term of  $C(s-b, t-1, n)$  via multiplying and dividing  $x_i$ 
         $x_i \leftarrow x_i \frac{u}{M}$ 
         $\ell_r \leftarrow \ell_r + x_i$ 
         $u \leftarrow u - (n+1)$ 
         $M \leftarrow M - (n+1)$ 

 $M'_{t-1} \leftarrow b$ 
 $\text{DCS}^+(t-1, n, s-b, M-\ell_l, M')$ 
return  $M'$ 

```

Unranking performance for $m = 256$

Algorithms are implemented in C/C++ with the **GMP library**.



Conclusion

We discussed some modifications to integer compositions that make their enumeration and generation harder.

We showed an instance of integer compositions appearing in the Winternitz one-time signature scheme.

We replaced its underlying “base- w ” unranking function by a more predictable, but slower alternative based on compositions.

We are currently looking into more efficient methods to unrank such restricted compositions via probabilistic methods and using other orders (e.g. minimal change).

References I

- [Ege13] Steffen Eger. Stirling's Approximation for Central Extended Binomial Coefficients. *Journal of Integer Sequences*, 16(13.1.3), 2013.
- [HBG⁺18] Andreas Hülsing, Denis Butin, Stefan-Lukas Gazdag, Joost Rijneveld, and Aziz Mohaisen. XMSS: Extended Hash-Based Signatures. Request for Comments 8391, Internet Engineering Task Force, May 2018.
- [PZC⁺21] Lucas Pandolfo Perin, Gustavo Zambonin, Ricardo Custódio, Lucia Moura, and Daniel Panario. Improved constant-sum encodings for hash-based signatures. *Journal of Cryptographic Engineering*, 11(1), May 2021.