Some properties of modular addition

Victoria Vysotskaya

JSC "InfoTeCS"

CTCrypt'18 / May 28, 2018

vysotskaya.victory@gmail.com

Definitions

Let us consider function $\boxplus_n$ meaning addition modulo 2^n. We also introduce the function $\Delta f(x, y, \Delta x)$:

$$\Delta f = \left[(x \oplus \Delta x) \boxplus_n y\right] \oplus (x \boxplus_n y).$$

Let us count all pairs (x, y) satisfying the equation for fixed $\Delta x, \Delta f$ and denote number of them $\varphi(\Delta x, \Delta f)$.

Definition

The table P_n of shape $2^n \times 2^n$ indexed by Δx and Δf with elements $(P_n)_{\Delta x, \Delta f} = \varphi(\Delta x, \Delta f)$ is called *Differential Distribution Table (DDT)*.

DDT has the following form

$$P_n = \begin{array}{c|ccccc} \Delta x \backslash \Delta f & 0 & \dots & \beta & \dots & 2^n-1 \\ \hline 0 & \ddots & & \vdots & & \\ \vdots & & \ddots & \vdots & & \\ \alpha & \dots & \dots & \varphi(\alpha,\beta) & & \\ \vdots & & & & & \\ 2^n-1 & & & & & \end{array}$$

$$\varphi(\alpha,\beta) = \left| \left\{ (x,y) : \beta = \left[(x \oplus \alpha) \boxplus_n y \right] \oplus (x \boxplus_n y) \right\} \right|.$$

Definition

Two rows of DDT are called *equivalent* if they coincide up to a permutation of their elements.

Problem statement

Question 1

How can we describe the equivalence classes?

Question 2

Can we efficiently describe the equivalence class a row with a given index belongs to?

Question 3

How many classes are there in matrix P_n?

Question 4

Can we generate all classes by the number n?

Theorem

Let matrix P_n have the form

$$P_n = \begin{bmatrix} A & B \\ C & D \end{bmatrix}.$$

Then matrix P_{n+1} has the form

$$P_{n+1} = 2 \left[\begin{array}{cc|cc} 2A & B & 0 & B \\ C & D & C & D \\ \hline 0 & B & 2A & B \\ C & D & C & D \end{array}\right].$$

Example

For $n = 1$

$$P_1 = 4 \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

For $n = 2$

$$P_2 = 8 \left[\begin{array}{cc|cc} 2 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ \hline 0 & 0 & 2 & 0 \\ 0 & 1 & 0 & 1 \end{array}\right].$$

Lemma

Let us define for each $n \geq 2$

$$A_n = \begin{bmatrix} 2A_{n-1} & B_{n-1} \\ B_{n-1} & A_{n-1} \end{bmatrix}, \quad B_n = \begin{bmatrix} 0 & B_{n-1} \\ B_{n-1} & A_{n-1} \end{bmatrix}$$

and $A_1 = \begin{bmatrix} 1 \end{bmatrix}$, $B_1 = \begin{bmatrix} 0 \end{bmatrix}$, *then*

$$P_n = 2^{n+1} \begin{bmatrix} A_n & B_n \\ B_n & A_n \end{bmatrix}.$$

Lemma

Only powers of two and zeros are elements of matrices A_n, B_n, P_n.

Now we want to construct an object so that there is a bijection between the objects and equivalence classes.

Idea

Let us consider an arbitrary row vector r of length 2^n with elements from the set $\{0, 1, 2, 4, \ldots, 2^{n-1}\}$. The vector $(k_0, k_1, \ldots, k_{n-1})$, where k_i is the number of occurrences of 2^i in vector r, is called a counter vector.

Example

$(0, 2, 0, 1, 0, 0, 0, 1) \mapsto (2, 1, 0)$,
$(4, 0, 0, 0, 0, 0, 0, 0) \mapsto (0, 0, 1)$.

Now we want to construct an object so that there is a bijection between the objects and equivalence classes.

Idea

Let us consider an arbitrary row vector r of length 2^n with elements from the set $\{0, 1, 2, 4, \ldots, 2^{n-1}\}$. The vector $(k_0, k_1, \ldots, k_{n-1})$, where k_i is the number of occurrences of 2^i in vector r, is called a counter vector.

Example

$(0, 2, 0, 1, 0, 0, 0, 1) \mapsto (2, 1, 0)$,
$(4, 0, 0, 0, 0, 0, 0, 0) \mapsto (0, 0, 1)$.

Now we want to construct an object so that there is a bijection between the objects and equivalence classes.

Idea

Let us consider an arbitrary row vector r of length 2^n with elements from the set $\{0, 1, 2, 4, \ldots, 2^{n-1}\}$. The vector $(k_0, k_1, \ldots, k_{n-1})$, where k_i is the number of occurrences of 2^i in vector r, is called a counter vector.

Example

$(0, 2, 0, 1, 0, 0, 0, 1) \mapsto (2, 1, 0)$,
$(4, 0, 0, 0, 0, 0, 0, 0) \mapsto (0, 0, 1)$.

Now we want to construct an object so that there is a bijection between the objects and equivalence classes.

Idea

Let us consider an arbitrary row vector r of length 2^n with elements from the set $\{0, 1, 2, 4, \ldots, 2^{n-1}\}$. The vector $(k_0, k_1, \ldots, k_{n-1})$, where k_i is the number of occurrences of 2^i in vector r, is called a counter vector.

Example

$(0, 2, 0, 1, 0, 0, 0, 1) \mapsto (2, 1, 0)$,
$(4, 0, 0, 0, 0, 0, 0, 0) \mapsto (0, 0, 1)$.

Idea

Let us match each row to a formal polynomial $p_r(x) = k_0 + k_1 x + k_2 x^2 + \cdots + k_{n-1} x^{n-1}$, *so that* $(k_0, k_1, k_2, \ldots, k_{n-1})$ *is the counter vector for this row.*

Then

$$p_{2r}(x) = x p_r(x),$$

$$p_{r||s}(x) = p_r(x) + p_s(x),$$

where symbol $||$ denotes concatenation of rows.
Now for i-th row

$$p_{n,i}(x) = x^{n+1}(a_{n,i}(x) + b_{n,i}(x)).$$

Recall that

$$A_n = \begin{bmatrix} 2A_{n-1} & B_{n-1} \\ B_{n-1} & A_{n-1} \end{bmatrix}, \quad B_n = \begin{bmatrix} 0 & B_{n-1} \\ B_{n-1} & A_{n-1} \end{bmatrix}.$$

Then the required polynomials have the following form:

$$a_{n,i}(x) = \begin{cases} xa_{n-1,i}(x) + b_{n-1,i}(x), & \text{if } \alpha_{n-2} = 0, \\ a_{n-1,i}(x) + b_{n-1,i}(x), & \text{if } \alpha_{n-2} = 1, \end{cases}$$

$$b_{n,i}(x) = \begin{cases} b_{n-1,i}(x), & \text{if } \alpha_{n-2} = 0, \\ a_{n-1,i}(x) + b_{n-1,i}(x), & \text{if } \alpha_{n-2} = 1, \end{cases}$$

where α_j is the j-th bit of binary representation of number i.

Lemma

$$p_{n,i}(x) = 2^{K-s+1} x^{n+1} \prod_{j=1}^{s-1} (x^{\ell_j} + x^{\ell_j - 1} + \cdots + 2) x^{\ell_s},$$

where

- *K is a number of 1's in binary representation of number i,*
- *s is a number of maximal disjoint groups of form $(1, \ldots, 1, 0, \ldots, 0)$ in binary representation of number i,*
- *ℓ_j is the number of 0's in j-th group.*

Lemma

$$p_{n,i}(x) = 2^{K-s+1} x^{n+1} \prod_{j=1}^{s-1} (x^{\ell_j} + x^{\ell_j - 1} + \cdots + 2) x^{\ell_s},$$

where

- *K is a number of 1's in binary representation of number i,*
- *s is a number of maximal disjoint groups of form $(1, \ldots, 1, 0, \ldots, 0)$ in binary representation of number i,*
- *ℓ_j is the number of 0's in j-th group.*

Example

$n = 7,\ i = 39 = (1, 0, 0, 1, 1, 1)$.

Lemma

$$p_{n,i}(x) = 2^{K-s+1} x^{n+1} \prod_{j=1}^{s-1} (x^{\ell_j} + x^{\ell_j - 1} + \cdots + 2) x^{\ell_s},$$

where

- *K is a number of 1's in binary representation of number i, $K = 4$.*
- *s is a number of maximal disjoint groups of form $(1, \ldots, 1, 0, \ldots, 0)$ in binary representation of number i,*
- *ℓ_j is the number of 0's in j-th group.*

Example

$n = 7,\ i = 39 = (1, 0, 0, 1, 1, 1)$.

Lemma

$$p_{n,i}(x) = 2^{K-s+1} x^{n+1} \prod_{j=1}^{s-1} (x^{\ell_j} + x^{\ell_j - 1} + \cdots + 2) x^{\ell_s},$$

where

- *K is a number of 1's in binary representation of number i, $K = 4$.*
- *s is a number of maximal disjoint groups of form $(1, \ldots, 1, 0, \ldots, 0)$ in binary representation of number i, $s = 2$.*
- *ℓ_j is the number of 0's in j-th group.*

Example

$n = 7,\ i = 39 = (1, 0, 0, 1, 1, 1, (0))$.

Lemma

$$p_{n,i}(x) = 2^{K-s+1} x^{n+1} \prod_{j=1}^{s-1} (x^{\ell_j} + x^{\ell_j - 1} + \cdots + 2) x^{\ell_s},$$

where

- *K is a number of 1's in binary representation of number i, $K = 4$.*
- *s is a number of maximal disjoint groups of form $(1, \ldots, 1, 0, \ldots, 0)$ in binary representation of number i, $s = 2$.*
- *ℓ_j is the number of 0's in j-th group. $\ell_1 = 2, \ell_2 = 0$.*

Example

$n = 7,\ i = 39 = (1, 0, 0, 1, 1, 1, (0))$.

Lemma

$$p_{n,i}(x) = 2^{K-s+1}x^{n+1}\prod_{j=1}^{s-1}(x^{\ell_j} + x^{\ell_j-1} + \cdots + 2)x^{\ell_s},$$

where

- *K is a number of 1's in binary representation of number i, $K = 4$.*
- *s is a number of maximal disjoint groups of form $(1, \ldots, 1, 0, \ldots, 0)$ in binary representation of number i, $s = 2$.*
- *ℓ_j is the number of 0's in j-th group. $\ell_1 = 2, \ell_2 = 0$.*

Example

$n = 7,\ i = 39 = (1, 0, 0, 1, 1, 1)$.
$p_{7,39}(x) = 2^{4-2+1}x^8(x^2 + x + 2) = 8x^{10} + 8x^9 + 16x^8$.

Lemma

$$p_{n,i}(x) = 2^{K-s+1}x^{n+1}\prod_{j=1}^{s-1}(x^{\ell_j} + x^{\ell_j-1} + \cdots + 2)x^{\ell_s},$$

where

- *K is a number of 1's in binary representation of number i,*
- *s is a number of maximal disjoint groups of form $(1, \ldots, 1, 0, \ldots, 0)$ in binary representation of number i,*
- *ℓ_j is the number of 0's in j-th group.*

Lemma

If $p_{n,d'}(x) = p_{n,d''}(x)$, then $K' = K''$, $s' = s''$, $\ell'_s = \ell''_s$ and multisets $\{\ell'_1, \ldots, \ell'_{s'-1}\}$ and $\{\ell''_1, \ldots, \ell''_{s''-1}\}$ are equal.

Lemma

$$p_{n,i}(x) = 2^{K-s+1} x^{n+1} \prod_{j=1}^{s-1} (x^{\ell_j} + x^{\ell_j - 1} + \cdots + 2) x^{\ell_s},$$

where

- *K is a number of 1's in binary representation of number i,*
- *s is a number of maximal disjoint groups of form $(1, \ldots, 1, 0, \ldots, 0)$ in binary representation of number i,*
- *ℓ_j is the number of 0's in j-th group.*

Definition

Q_n is a set of tuples $\left(K, s, \ell_s, \{\ell_1, \ldots, \ell_{s-1}\}\right)$ corresponding to numbers $i \in \{0, \ldots, 2^{n-1} - 1\}$.

Theorem

There exists a one-to-one correspondence between the set of equivalence classes of the matrix P_n rows and the parameter set Q_n.

Note

To enumerate all the equivalence classes it is sufficient to iterate over all the tuples from Q_n. Thus they can be generated in time proportional to number of non-equivalent rows of matrix P_n. On the contrary, the brute-force algorithm requires time proportional to number of all matrix rows.

Definition

Let $p(n,k)$ denote the number of partitions of n into exactly k parts and $p(n) = \sum_{s=1}^{n} p(n,s)$.

Example

Table: Partitions for $n = 5$

k	1	2	3	4	5
$p(n,k)$	1	2	2	1	1
partitions	$\{5\}$	$\{3,2\}$, $\{4,1\}$	$\{3,1,1\}$, $\{2,2,1\}$	$\{2,1,1,1\}$	$\{1,1,1,1,1\}$

$$p(5) = p(5,1) + p(5,2) + p(5,3) + p(5,4) + p(5,5) = 1 + 2 + 2 + 1 + 1 = 7.$$

Lemma

$$p(n,k) = p(n-1,k-1) + p(n-k,k).$$

Theorem

$$|Q_n| = \sum_{j=1}^{n-1} p(j) + 1, \ \ n > 3.$$

Lemma

$$p(n,k) = p(n-1,k-1) + p(n-k,k).$$

Theorem

$$|Q_n| = \sum_{j=1}^{n-1} p(j) + 1, \ \ n > 3.$$

Note

Now we see that the complexity of computing $|Q_n|$ is $O(n^3)$ bit operations.

Theorem

$$|Q_n| = \sum_{j=1}^{n-1} p(j) + 1, \ \ n > 3.$$

Hardy and Ramanujan obtained an estimate:

$$p(n) \sim \frac{1}{4\sqrt{3}n} e^{\pi\sqrt{\frac{2n}{3}}} \text{ as } n \to \infty$$

using which we proved

Theorem

$$|Q_n| \sim \frac{e^{\pi\sqrt{\frac{2n}{3}}}}{2\sqrt{2}\pi\sqrt{n}} \text{ as } n \to \infty.$$

Theorem

$$|Q_n| \sim \frac{e^{\pi\sqrt{\frac{2n}{3}}}}{2\sqrt{2}\pi\sqrt{n}} \text{ as } n \to \infty.$$

Corollary

$$|Q_n| = 2^{O(\sqrt{n})} \text{ as } n \to \infty.$$

Note

Now we can claim we can enumerate all the equivalence classes in $2^{O(\sqrt{n})}$ bit operation.

Conclusion

In this work we

1. obtained a general formula for representation of introduced equivalence classes in DDT;
2. provided an efficient method for computing the representation of the equivalence class of a row with a given index;
3. obtained an exact formula for the number of equivalence classes;
4. proved an asymptotically accurate approximation of number of equivalence classes;
5. sketched an algorithm to generate all equivalence classes in $2^{O(\sqrt{n})}$ bit operations.

Questions?