

Attacking algorithm for $\mathcal{H}(2, 0^k)$

2024-08-04

0.1 Data

Suppose we have a translation surface (X, ω) with n_1 short cylinders and n_2 long cylinders with some label, either A or B . I will call them $C_0, \dots, C_{n_1}, C_{n_1+1}, \dots, C_{n_1+n_2-1}$ (sorry about the 0-indexing!). Let the height of C_i be c_i .

For cylinders $C_{n_1+1}, C_{n_1+2}, C_{n_1+n_2-2}, C_{n_1+n_2-1}$ (excluding cases where any of these indices are $n_1, n_1 + n_2$) we associate an array $\text{marked}_i[]$ which is a nonempty subset of $\{\ell, r\}$, denoting whether there is a marked point on the left and/or right half on top of cylinder C_i .

0.2 The algorithm

- I can assume that $n_1, n_2 \geq 2$ because otherwise no vertically-scaling rel deformations exist
- With this email, (I think) I can eliminate *all* cases where there are 3 cylinders of the same label in a row. Therefore, any attack (top or bottom) comes from at most 2 cylinders in $\mathcal{H}(2, 0^k)$.

0.2.1 Attacks from the bottom

For every cylinder C_i (most of the time) we compute the attack below it as:

- (1) $c_{i+2} + c_{i+1}$ (indices are taken mod($n_1 + n_2$)) if the label of C_{i+2} and C_{i+1} is different from C_i ,
- (2) otherwise, c_{i+1} if the label of C_{i+1} is not C_i
- (3) otherwise, 0

There is a special cases though when C_i is a short cylinder and C_{i+1} or C_{i+2} are long cylinders.

- (1) If C_i is a short cylinder and C_{i+1} and C_{i+2} are long cylinders (this means $i = n_1 - 1$):
 - (a) $c_{i+1} + c_{i+2}$ if C_{i+1} and C_{i+2} have different labels to C_i and $\ell \in \text{marked}_{n_1+3}$ (its important that AA/BB on the bottom is impossible, because otherwise marked_{n_1+3} does not exist!).
 - (b) otherwise, c_{i+1} if C_{i+1} has a different label than C_i and $\ell \in \text{marked}_{n_1+2}$
 - (c) otherwise, 0
- (2) If C_i and C_{i+1} are short cylinders and C_{i+2} is a long cylinder (this means $i = n_1 - 2$):
 - (a) $c_{i+1} + c_{i+2}$ if C_{i+1} and C_{i+2} have different labels to C_i and $\ell \in \text{marked}_{n_1+2}$.
 - (b) otherwise, c_{i+1} if C_{i+1} has a different label than C_i
 - (c) otherwise, 0

There is another special case where C_i is one of the bottom two cylinders ($i = n_1 + n_2 - 1$ or $i = n_1 + n_2 - 2$).

- (1) If $i = n_1 + n_2 - 1$ then the attack is
 - (a) $c_{n_1} + c_{n_1+1}$ if C_{n_1} and C_{n_1+1} have different labels to C_i and $r \in \text{marked}_{n_1+2}$ (again, it's important that AA/BB on the bottom is impossible).

- (b) otherwise, c_{n_1} if C_{n_1} has a different label than C_i and $r \in \text{marked}_{n_1+1}$
- (c) otherwise, 0
- (2) If $i = n_1 + n_2 - 2$ then the attack is
 - (a) $c_{n_1+n_2-1} + c_{n_1}$ if $C_{n_1+n_2-1}$ and C_{n_1} have different labels to C_i and $r \in \text{marked}_{n_1+1}$
 - (b) otherwise, $c_{n_1+n_2-1}$ if $C_{n_1+n_2-1}$ has a different label than C_i
 - (c) otherwise, 0

0.2.2 Attacks from the top

This is similar to the bottom.

For every cylinder C_i (most of the time) we compute the attack above it as:

- (1) $c_{i-2} + c_{i-1}$ if the label of C_{i-2} and C_{i-1} is different from C_i ,
- (2) otherwise, c_{i-1} if the label of C_{i-1} is not C_i
- (3) otherwise, 0

There is a special cases though when C_i is a short cylinder and C_{i+1} or C_{i+2} are long cylinders (this is $i = 0, 1$).

- (1) If C_0 is a short cylinder and $C_{n_1+n_2-1}$ and $C_{n_1+n_2-2}$ are long cylinders:
 - (a) $c_{n_1+n_2-1} + c_{n_1+n_2-2}$ if $C_{n_1+n_2-1}$ and $C_{n_1+n_2-2}$ have different labels to C_0 and $\ell \in \text{marked}_{n_1+n_2-2}$ (its important that AA/BB on the bottom is impossible again because in this case $n_1 + n_2 - 2 = n_1$).
 - (b) otherwise, $c_{n_1+n_2-1}$ if $C_{n_1+n_2-1}$ has a different label than C_0 and $\ell \in \text{marked}_{n_1+n_2-1}$
 - (c) otherwise, 0
- (2) If C_1 and C_0 are a short cylinders and $C_{n_1+n_2-1}$ is a long cylinder:
 - (a) $c_0 + c_{n_1+n_2-1}$ if C_0 and $C_{n_1+n_2-1}$ have different labels to C_1 and $\ell \in \text{marked}_{n_1+n_2-1}$.
 - (b) otherwise, c_{i+1} if C_{i+1} has a different label than C_i
 - (c) otherwise, 0

There is another special case where C_i is one of the top two long cylinders ($i = n_1$ or $i = n_1 + 1$).

- (1) If $i = n_1$ then the attack is
 - (a) $c_{n_1+n_2-1} + c_{n_1+n_2-2}$ if $C_{n_1+n_2-1}$ and $C_{n_1+n_2-2}$ have different labels to C_i and $r \in \text{marked}_{n_1+n_2-2}$ (again, it's important that AA/BB on the bottom is impossible).
 - (b) otherwise, $c_{n_1+n_2-1}$ if $C_{n_1+n_2-1}$ has a different label than C_i and $r \in \text{marked}_{n_1+n_2-1}$
 - (c) otherwise, 0
- (2) If $i = n_1 + 1$ then the attack is
 - (a) $c_{n_1+n_2-1} + c_{n_1}$ if $C_{n_1+n_2-1}$ and C_{n_1} have different labels to C_i and $r \in \text{marked}_{n_1+1}$
 - (b) otherwise, c_{n_1+1} if C_{n_1+1} has a different label than C_i
 - (c) otherwise, 0

0.3 How many equations?

Since each marked_i can be either $\{\ell\}$, $\{r\}$, $\{\ell + r\}$, this gives up to $3^4 = 81$ times more equations to solve. On the other hand, sometimes $\text{marked}_{n_1+1} = \{\ell, r\}$, $\text{marked}_{n_1+2} = \{r\}$ is the same as $\text{marked}_{n_1+1} = \{\ell\}$, $\text{marked}_{n_1+2} = \{r\}$. There might be some simplification in most cases then.