Coppersmith / Howgrave-Graham and LLL

Tanja Lange

Eindhoven University of Technology

22 September 2020

Theorem by Howgrave-Graham

Let $g(x) = \sum_{i=0}^{d-1} g_i x^i \in \mathbf{Z}[x]$ of $\deg(g) = d - 1$.
Let $m, b \in \mathbf{Z}_{>0}$
If

1. $g(x_0) \equiv 0 \bmod b^m$ with $|x_0| \leq X$,
2. $||g(xX)|| \leq b^m/\sqrt{d}$

then $g(x_0) = 0$ over $\mathbf{Z}$.
Here $||g(xX)|| = \sqrt{g_0^2 + g_1^2 X^2 + \cdots + g_{d-1}^2 X^{2(d-1)}}$ is the Euclidean norm of the coefficient vector of $g(xX)$.

Theorem by Howgrave-Graham

Let $g(x) = \sum_{i=0}^{d-1} g_i x^i \in \mathbf{Z}[x]$ of $\deg(g) = d-1$.
Let $m, b \in \mathbf{Z}_{>0}$
If

1. $g(x_0) \equiv 0 \bmod b^m$ with $|x_0| \leq X$,
2. $||g(xX)|| \leq b^m/\sqrt{d}$

then $g(x_0) = 0$ over $\mathbf{Z}$.
Here $||g(xX)|| = \sqrt{g_0^2 + g_1^2 X^2 + \cdots + g_{d-1}^2 X^{2(d-1)}}$ is the Euclidean norm of the coefficient vector of $g(xX)$.

If $x_0 \equiv 0 \bmod b^m$ and $|x_0| < b^m$ then

Theorem by Howgrave-Graham

Let $g(x) = \sum_{i=0}^{d-1} g_i x^i \in \mathbf{Z}[x]$ of $\deg(g) = d - 1$.
Let $m, b \in \mathbf{Z}_{>0}$
If

1. $g(x_0) \equiv 0 \bmod b^m$ with $|x_0| \leq X$,
2. $||g(xX)|| \leq b^m/\sqrt{d}$

then $g(x_0) = 0$ over $\mathbf{Z}$.
Here $||g(xX)|| = \sqrt{g_0^2 + g_1^2 X^2 + \cdots + g_{d-1}^2 X^{2(d-1)}}$ is the Euclidean norm of the coefficient vector of $g(xX)$.

If $x_0 \equiv 0 \bmod b^m$ and $|x_0| < b^m$ then $x_0 = 0$.

Theorem by Howgrave-Graham

Let $g(x) = \sum_{i=0}^{d-1} g_i x^i \in \mathbf{Z}[x]$ of $\deg(g) = d - 1$.
Let $m, b \in \mathbf{Z}_{>0}$
If

1. $g(x_0) \equiv 0 \bmod b^m$ with $|x_0| \leq X$,
2. $||g(xX)|| \leq b^m/\sqrt{d}$

then $g(x_0) = 0$ over $\mathbf{Z}$.
Here $||g(xX)|| = \sqrt{g_0^2 + g_1^2 X^2 + \cdots + g_{d-1}^2 X^{2(d-1)}}$ is the Euclidean norm of the coefficient vector of $g(xX)$.

If $x_0 \in b^m\mathbf{Z}$ and $|x_0| < b^m$ then $x_0 = 0$.

Theorem by Howgrave-Graham

Let $g(x) = \sum_{i=0}^{d-1} g_i x^i \in \mathbf{Z}[x]$ of $\deg(g) = d - 1$.
Let $m, b \in \mathbf{Z}_{>0}$
If

1. $g(x_0) \equiv 0 \bmod b^m$ with $|x_0| \leq X$,
2. $||g(xX)|| \leq b^m/\sqrt{d}$

then $g(x_0) = 0$ over $\mathbf{Z}$.
Here $||g(xX)|| = \sqrt{g_0^2 + g_1^2 X^2 + \cdots + g_{d-1}^2 X^{2(d-1)}}$ is the Euclidean norm of the coefficient vector of $g(xX)$.

If $x_0 \in b^m\mathbf{Z}$ and $|x_0| < b^m$ then $x_0 = 0$.
If $g(x_0) \in b^m\mathbf{Z}$ and $|g(x_0)| < b^m$ then $g(x_0) = 0$.

Theorem by Howgrave-Graham

Let $g(x) = \sum_{i=0}^{d-1} g_i x^i \in \mathbf{Z}[x]$ of $\deg(g) = d - 1$.
Let $m, b \in \mathbf{Z}_{>0}$
If

1. $g(x_0) \equiv 0 \bmod b^m$ with $|x_0| \leq X$,
2. $||g(xX)|| \leq b^m/\sqrt{d}$

then $g(x_0) = 0$ over $\mathbf{Z}$.
Here $||g(xX)|| = \sqrt{g_0^2 + g_1^2 X^2 + \cdots + g_{d-1}^2 X^{2(d-1)}}$ is the Euclidean norm of the coefficient vector of $g(xX)$.

If $x_0 \in b^m\mathbf{Z}$ and $|x_0| < b^m$ then $x_0 = 0$.
If $g(x_0) \in b^m\mathbf{Z}$ and $|g(x_0)| < b^m$ then $g(x_0) = 0$.
Putting in bound on x_0 and expanding the absolute value.
If $g(x_0) \in b^m\mathbf{Z}, |x_0| < X, |g_0| \leq b^m/d, |g_1 X| \leq b^m/d,$
$|g_2 X^2| \leq b^m/d, \ldots, |g_{d-1} X^{d-1}| \leq b^m/d$ then $g(x_0) = 0$.

Theorem by Howgrave-Graham

Let $g(x) = \sum_{i=0}^{d-1} g_i x^i \in \mathbf{Z}[x]$ of $\deg(g) = d - 1$.
Let $m, b \in \mathbf{Z}_{>0}$
If

1. $g(x_0) \equiv 0 \bmod b^m$ with $|x_0| \leq X$,
2. $||g(xX)|| \leq b^m/\sqrt{d}$

then $g(x_0) = 0$ over $\mathbf{Z}$.
Here $||g(xX)|| = \sqrt{g_0^2 + g_1^2 X^2 + \cdots + g_{d-1}^2 X^{2(d-1)}}$ is the Euclidean norm of the coefficient vector of $g(xX)$.

If $x_0 \in b^m\mathbf{Z}$ and $|x_0| < b^m$ then $x_0 = 0$.
If $g(x_0) \in b^m\mathbf{Z}$ and $|g(x_0)| < b^m$ then $g(x_0) = 0$.
Putting in bound on x_0 and expanding the absolute value.
If $g(x_0) \in b^m\mathbf{Z}, |x_0| < X, |g_0| \leq b^m/d, |g_1 X| \leq b^m/d$,
$|g_2 X^2| \leq b^m/d, \ldots, |g_{d-1}X^{d-1}| \leq b^m/d$ then $g(x_0) = 0$.

Now just square, sum up and take the squre root on both sides:
$\sum_{i=0}^{d-1} g_i^2 X^{2i} \leq \sum_{i=0}^{d-1} b^{2m}/d^2 = b^{2m}/d$.

What to look for?

We want to find a polynomial $g(x)$ and a root x_0 so that $g(x_0) \in b^m\mathbf{Z}$.

What to look for?

We want to find a polynomial $g(x)$ and a root x_0 so that $g(x_0) \in b^m\mathbf{Z}$.
Here are some polynomials that work:
$g(x) \in b^m\mathbf{Z} + b^m x\mathbf{Z}$

What to look for?

We want to find a polynomial $g(x)$ and a root x_0 so that $g(x_0) \in b^m\mathbf{Z}$.
Here are some polynomials that work:
$g(x) \in b^m\mathbf{Z} + b^m x\mathbf{Z} + b^m x^2\mathbf{Z}$

What to look for?

We want to find a polynomial $g(x)$ and a root x_0 so that $g(x_0) \in b^m\mathbf{Z}$.
Here are some polynomials that work:
$g(x) \in b^m\mathbf{Z} + b^m x\mathbf{Z} + b^m x^2\mathbf{Z} + b^m x^3\mathbf{Z} \cdots$.

What to look for?

We want to find a polynomial $g(x)$ and a root x_0 so that $g(x_0) \in b^m\mathbf{Z}$.
Here are some polynomials that work:
$g(x) \in b^m\mathbf{Z} + b^m x\mathbf{Z} + b^m x^2\mathbf{Z} + b^m x^3\mathbf{Z} \cdots$.

We have some polynomial $f(x)$ to start with and know that $f(x_0) \in b^m\mathbf{Z}$ for the x_0 we're looking for.

What to look for?

We want to find a polynomial $g(x)$ and a root x_0 so that $g(x_0) \in b^m\mathbf{Z}$.
Here are some polynomials that work:
$g(x) \in b^m\mathbf{Z} + b^m x\mathbf{Z} + b^m x^2\mathbf{Z} + b^m x^3\mathbf{Z} \cdots$.

We have some polynomial $f(x)$ to start with and know that $f(x_0) \in b^m\mathbf{Z}$ for the x_0 we're looking for.

If $\deg(f) = t$ then we're looking for
$g(x) \in b^m\mathbf{Z} + b^m x\mathbf{Z} + b^m x^2\mathbf{Z} + \cdots + b^m x^{t-1}\mathbf{Z} + f(x)\mathbf{Z}$.
The polynomial f takes care of the b^m for x^t.

What to look for?

We want to find a polynomial $g(x)$ and a root x_0 so that $g(x_0) \in b^m\mathbf{Z}$.
Here are some polynomials that work:
$g(x) \in b^m\mathbf{Z} + b^m x\mathbf{Z} + b^m x^2\mathbf{Z} + b^m x^3\mathbf{Z} \cdots$.

We have some polynomial $f(x)$ to start with and know that $f(x_0) \in b^m\mathbf{Z}$ for the x_0 we're looking for.

If $\deg(f) = t$ then we're looking for
$g(x) \in b^m\mathbf{Z} + b^m x\mathbf{Z} + b^m x^2\mathbf{Z} + \cdots + b^m x^{t-1}\mathbf{Z} + f(x)\mathbf{Z}$.
The polynomial f takes care of the b^m for x^t.

If that's too restrictive we can expand to
$g(x) \in$
$b^m\mathbf{Z} + b^m x\mathbf{Z} + b^m x^2\mathbf{Z} + \cdots + b^m x^{t-1}\mathbf{Z} + f(x)\mathbf{Z} + xf(x)\mathbf{Z} + x^2 f(x)\mathbf{Z} + \cdots$.

What to look for and how to find it?

All of these attacks start by finding sme polynomial $\deg(f) = t$ for which we a root modulo b^m is intersting. Let $\deg(f) = t$ and let $|x_0| \leq X$ for some known X.

To find
$g(x) \in$
$b^m\mathbf{Z} + b^m x\mathbf{Z} + b^m x^2\mathbf{Z} + \cdots + b^m x^{t-1}\mathbf{Z} + f(x)\mathbf{Z} + xf(x)\mathbf{Z} + x^2 f(x)\mathbf{Z} + \cdots$
we will use LLL, which builds integer linear combinations of the input rows of a matrix. It returns a vector that is short in the Euclidean norm. (Hence we wanted that in the Howgrave-Graham theorem).

We set up a system of equations in the coeffient vectors, one row per option. $b^m\mathbf{Z}$ turns into coefficient b^m at the x^0 column etc.

For Howgrave-Graham we need to scale the column of x^s by X^s. So we get

$$\begin{pmatrix} X & a \\ 0 & n \end{pmatrix}$$

for knowing part of p.

What to look for and how to find it?

All of these attacks start by finding sme polynomial $\deg(f) = t$ for which we a root modulo b^m is intersting. Let $\deg(f) = t$ and let $|x_0| \leq X$ for some known X.

To find
$g(x) \in$
$b^m\mathbf{Z} + b^m x\mathbf{Z} + b^m x^2\mathbf{Z} + \cdots + b^m x^{t-1}\mathbf{Z} + f(x)\mathbf{Z} + xf(x)\mathbf{Z} + x^2 f(x)\mathbf{Z} + \cdots$
we will use LLL, which builds integer linear combinations of the input rows of a matrix. It returns a vector that is short in the Euclidean norm. (Hence we wanted that in the Howgrave-Graham theorem).

We set up a system of equations in the coeffient vectors, one row per option. $b^m\mathbf{Z}$ turns into coefficient b^m at the x^0 column etc.

For Howgrave-Graham we need to scale the column of x^s by X^s. So we get

$$\begin{pmatrix} X^2 & aX & 0 \\ 0 & X & a \\ 0 & 0 & n \end{pmatrix}$$

for knowing part of p.

What to look for and how to find it?

All of these attacks start by finding sme polynomial $\deg(f) = t$ for which we a root modulo b^m is intersting. Let $\deg(f) = t$ and let $|x_0| \leq X$ for some known X.

To find
$g(x) \in$
$b^m\mathbf{Z} + b^m x\mathbf{Z} + b^m x^2\mathbf{Z} + \cdots + b^m x^{t-1}\mathbf{Z} + f(x)\mathbf{Z} + xf(x)\mathbf{Z} + x^2 f(x)\mathbf{Z} + \cdots$
we will use LLL, which builds integer linear combinations of the input rows of a matrix. It returns a vector that is short in the Euclidean norm. (Hence we wanted that in the Howgrave-Graham theorem).

We set up a system of equations in the coeffient vectors, one row per option. $b^m\mathbf{Z}$ turns into coefficient b^m at the x^0 column etc.

For Howgrave-Graham we need to scale the column of x^s by X^s. So we get

$$\begin{pmatrix} X^2 & aX & 0 \\ 0 & X & a \\ 0 & 0 & n \end{pmatrix} \stackrel{?}{=} \begin{pmatrix} X^2 & 2aX & a^2 \\ 0 & X & a \\ 0 & 0 & n \end{pmatrix}$$

for knowing part of p.

LLL

Due to Lenstra, Lensra, and Lovász, 1982.

- On input a set of vectors $\{v_1, v_2, \ldots, v_d\}$ output a short vector v_1' so that $v_1' = \sum a_i v_i$ for some $a_i \in \mathbf{Z}$.

LLL

Due to Lenstra, Lensra, and Lovász, 1982.

- On input a set of vectors $\{v_1, v_2, \ldots, v_d\}$ output a short vector v'_1 so that $v'_1 = \sum a_i v_i$ for some $a_i \in \mathbf{Z}$.
- LLL outputs d vectors which are shorter and more orthogonal. Each vector is an integer linear combinantion of the inputs.
- LLL uses many elements from Gram-Schmidt orthogonalization:
  - for $j = 1$ to d
  - for $i = 1$ to $j - 1$
  - $\mu_{ij} = \frac{\langle v_i^*, v_j \rangle}{\langle v_i^*, v_i^* \rangle}$
  - $v_j^* = v_j - \sum_{i=1}^{j-1} \mu_{ij} v_i^*$
- Note that the μ_{ij} are not integers, so the v_j^* are not in the lattice.
- A lattice basis is LLL reduced for parameter $0.25 < \delta < 1$ if
  - $|\mu_{ij}| \leq 0.5$ for all $1 \leq j < i \leq d$,
  - $(\delta - \mu_{i-1i}^2)||v_{i-1}^*||^2 \leq ||v_i^*||^2$.
- This guarantees $||v_1|| \leq (2/\sqrt{4\delta - 1})^{(d-1)/2} \det(L)^{1/d}$, where $\det(L)$ is the determinant of the lattice.

LLL algorithm (from Cohen, GTM 138, transposed)

Input: Basis $\{v_1, v_2, \ldots, v_d\}$ of lattice L, $0.25 < \delta < 1$
Output: LLL reduced basis for L with parameter δ

1. $k \leftarrow 2,\ k_{\max} \leftarrow 1,\ v_1^* \leftarrow v_1,\ V_1 = \langle v_1, v_1 \rangle$
2. if $k \leq k_{\max}$ go to step 3
   else $k_{\max} \leftarrow k,\ v_k^* \leftarrow v_k$, for $j = 1$ to $k - 1$
   - put $\mu_{jk} \leftarrow \langle v_j^*, v_k \rangle / V_j$ and $v_k^* \leftarrow v_k^* - \mu_{jk} v_j^*$

   $V_k = \langle v_k, v_k \rangle$
3. Execute RED$(k, k-1)$. If $(\delta - \mu_{i-1i}^2) V_{k-1} > V_k$ execute SWAP(k) and $k \leftarrow \max\{2, k-1\}$; else for $= k - 2$ down to 1 execute RED(k, j) and $k \leftarrow k + 1$.
4. If $k \leq d$ go to step 2; else output basis $\{v_1, v_2, \ldots, v_d\}$.

- RED(k, j): If $|\mu_{jk}| \leq 0.5$ return; else $q \leftarrow \lfloor \mu_{jk} \rceil$, $v_k \leftarrow v_k - q v_j$, $\mu_{jk} \leftarrow \mu_{jk} - q$, for $i = 1$ to $j - 1$ put $\mu_{ik} \leftarrow \mu_{ik} - q\mu_{ij}$ and return.
- SWAP(k): Swap v_k and v_{k-1}. If $k > 2$ for $j = 1$ to $k - 2$ swap μ_{jk} and μ_{jk-1} and update all variables to match (see p.88 in Cohen)

For a nice visualization see pages 61–66 of
http://thijs.com/docs/lec1.pdf.
(Animations only work in acroread.)