Op zoek naar goede ABC-hits (2)

Johan Bosman

(aantekeningen: Jeanine Daems)

De methode die we hier bespreken is geïntroduceerd door Benne de Weger in 1986.

De definities zijn hetzelfde als in de voordracht *Op zoek naar goede ABC-hits (1)* door Jaap Top, namelijk: een drietal positieve gehele getallen a, b en c heet een *ABC-drietal* als a en b onderling ondeelbaar zijn, a kleiner is dan b en als $a + b = c$ geldt. Een ABC-drietal heet een *ABC-hit* als $\mathrm{rad}(abc) < c$. Een ABC-hit heet een *goede ABC-hit* als de kwaliteit $\frac{\log(c)}{\log(\mathrm{rad}(abc))}$ minstens 1.4 is.

De methode om goede ABC-hits te vinden die we hier bespreken werkt als volgt. Kies een aantal kleine priemgetallen $p_1 \leq p_2 \leq \ldots \leq p_n$. Definieer de verzameling $S = \{p_1^{x_1} \cdot p_2^{x_2} \cdot \ldots \cdot p_n^{x_n} : x_1, \ldots, x_n \in \mathbb{Z}_{\geq 0}\}$. We zoeken naar drietallen a, b en c waarvoor geldt dat $b, c \in S$ en $a := c - b$ klein is.

We willen $\frac{\log(c)}{\log(\mathrm{rad}(abc))}$ maximaliseren, dus we gaan proberen om $\frac{\log(\mathrm{rad}(abc))}{log(c)}$ te minimaliseren. Merk op dat

$$\frac{\log(\mathrm{rad}(abc))}{\log(c)} = \frac{\log(\mathrm{rad}(a))}{\log(c)} + \frac{\log(\mathrm{rad}(bc))}{\log(c)} \leq \frac{\log(a)}{\log(c)} + \frac{\sum_{i=1}^{n} \log(p_i)}{\log(c)}.$$

De term $\frac{\sum_{i=1}^{n} \log(p_i)}{\log(c)}$ is klein. We willen dus $\frac{\log(a)}{\log(c)}$ minimaliseren. De uitspraak "$\frac{\log(a)}{\log(c)}$ is klein" betekent hetzelfde als "a is een kleine macht van c" of, equivalent, "a is een kleine macht van b". Denk dan bijvoorbeeld aan $a < b^{\delta}$, met $\delta = \frac{1}{2}$.

We willen $x_1, \ldots, x_n, y_1, \ldots, y_n \in \mathbb{Z}_{\geq 0}$ vinden zodanig dat $x_i \neq 0 \Rightarrow y_i = 0$ en $y_i \neq 0 \Rightarrow x_i = 0$. Dan definiëren we $c = p_1^{x_1} \cdot \ldots \cdot p_n^{x_n}$ en $b = p_1^{y_1} \cdot \ldots \cdot p_n^{y_n}$. Merk op dat de eis die we aan de x_i's en de y_i's hebben opgelegd ervoor zorgen dat b en c copriem zijn. Bovendien willen we dat $c - b = a$ klein is, dus $\frac{c}{b} = \frac{p_1^{x_1} \cdot \ldots \cdot p_n^{x_n}}{p_1^{y_1} \cdot \ldots p_n^{y_n}}$ zal dicht bij 1 moeten liggen. Definieer nu z_i voor $i = 1, \ldots, n$ door $\frac{c}{b} = p_1^{z_1} \cdot \ldots \cdot p_n^{z_n}$ met $z_i \in \mathbb{Z}$(dus $z_i = x_i - y_i$, en als z_i positief is, dan is $p_i^{z_i}$ een deler van c, en als z_i negatief is, dan is $p_i^{-z_i}$ een deler van b).

Als $\frac{c}{b} \approx 1$, dan geldt $\log(\frac{c}{b}) \approx 0$, oftewel $z_1 \log(p_1) + \ldots + z_n \log(p_n) \approx 0$. *Hoe* dicht willen we nu dat $z_1 \log(p_1) + \ldots + z_n \log(p_n) \approx 0$ bij 0 ligt? We willen dat $a < b^{\delta}$ voor een kleine $\delta \in \mathbb{R}$.

Merk op dat dan zou gelden:

$$\log(\frac{c}{b}) \approx \frac{c}{b} - 1 = \frac{c-b}{b} = \frac{a}{b} < \frac{b^{\delta}}{b} = \frac{1}{b^{1-\delta}},$$

dus we willen dat

$$|z_1 \log(p_1) + \ldots + z_n \log(p_n)| < \frac{1}{b^{1-\delta}}.$$

De term aan de linkerkant van deze ongelijkheid kan polynomiaal verlaagd worden, terwijl de term aan de rechterkant exponentieel kleiner wordt als we de z_i vergroten. We moeten dus kleine waarden van $\sum z_i \log(p_i)$ vinden zonder z_i te groot te laten worden.

Roosterreductie

Kies een constance $C \in \mathbb{R}_{>0}$. We maken de vectoren

$$\begin{aligned} v_1 &= (C \log(p_1), 1, 0, \ldots, 0) \\ v_2 &= (C \log(p_2), 0, 1, 0, \ldots, 0) \\ &\vdots \\ v_n &= (C \log(p_n), 0, \ldots, 0, 1). \end{aligned}$$

Beschouw nu het rooster $\Lambda = \{z_1 v_1 + \ldots z_n v_n : z_i \in \mathbb{Z}\}$. Elementen van Λ zijn van de vorm $v = z_1 v_1 + \ldots + z_n v_n = (C \cdot (z_1 \log(p_1) + \ldots + z_n \log(p_n)), z_1, \ldots, z_n)$. Als $|v|$ klein is, dan is $z_1 \log(p_1) + \ldots + z_n \log(p_n)$ klein en de z_i niet te groot. Dat is precies wat we willen. (Deze groottes hangen af van de waarde van C, maar het komt niet zo precies: als C werkt, dan werken $10C$ en $\frac{1}{10}C$ ook wel.)

Stel dat we zoeken met $n = 3$ en we proberen systematisch drietallen p_1, p_2, p_3. Dan zullen we het drietal $p_1 = 3$, $p_2 = 23$ en $p_3 = 109$ tegenkomen. Met $C = 5000$ vinden we dan:

$$\begin{aligned} v_1 &= (5493.1\ldots, 1, 0, 0) \\ v_2 &= (15677.5\ldots, 0, 1, 0) \\ v_3 &= (23456.7\ldots, 0, 0, 1) \end{aligned}$$

Als we nu het LLL-algoritme gebruiken om kleine vectoren te vinden, dat vinden we de basis:

$$\{(0.0016\ldots, -10, 5, -1), (30.826\ldots, 7, 17, -113), (26.457\ldots, -31, -43, 36)\}.$$

De basisvector $(0.0016\ldots, -10, 5, -1)$ levert ons een goede ABC-hit: $c = 23^5$, $b = 3^{10} \cdot 109$ en dus $a = 2$.

Kies een priemmacht p^e. We gaan nu drietallen a, b, c zoeken met $b, c \in S$ zodanig dat $p^e | c - b = a$. Schrijf nu a als $a = p^e \cdot a'$. Het doel is om a' klein te maken. We bekijken nu $(z_1, \ldots, z_n)$ waarvoor geldt dat $p_1^{z_1} \cdot \ldots \cdot p_n^{z_n} \equiv 1 \pmod{p^e}$. Dit betekent dat we in een deelrooster van Λ gaan kijken. Op deze manier vinden we ABC-drietallen die voldoen aan $a = p^e a'$, waarbij a' klein is.

Als C een goede waarde is om te gebruiken in het volledige rooster, dan werkt $\frac{C}{p^e}$ goed voor dit deelrooster.

Voorbeeld: Stel $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 11$, $p_5 = 31$ en $p^e = 196$. Dan bevat Λ de kleinste vector $(0.6328\ldots, 6, -27, 6, 9, 7)$, maar Λ bevat ook $(0.002, -30, 13, -1, 2, 1)$. Deze laatste vector geeft ons de goede ABC-hit $13 \cdot 19^6 + 2^{30} \cdot 5 = 3^{13} \cdot 11^2 \cdot 31$ met kwaliteit $q = 1.52700$.