Autoformalizating Siegel's lemma

April 30, 2024

Theorem 0.1 (Lemma 8.1)**.** *Let $0 < M < N$, and a_{jk} be rational integers satisfying*

$$|a_{jk}| \leq A \quad \text{where } 1 \leq A,\ 1 \leq j \leq M \text{ and } 1 \leq k \leq N. \tag{1}$$

Then there exists a set of rational integers $x_1..., x_N$, not all zero, satisfying

$$a_{j1}x_1 + \cdots a_{jN}x_N = 0,\ 1 \leq j \leq M \tag{2}$$

and

$$|x_k| \leq (NA)^{\frac{M}{N-M}},\ 1 \leq k \leq N. \tag{3}$$

Proof. Let

$$H = (NA)^{\frac{M}{N-M}}). \tag{4}$$

Then

$$NA < (H+1)^{(\frac{N-M}{M})}. \tag{5}$$

Hence

$$(NAH) + 1 \leq NA(H+1) \tag{6}$$

and

$$NA(H+1) < (H+1)^{\frac{N}{M}} \tag{7}$$

Define

$$y_j = a_{j1}x_1 + \cdots a_{jN}x_N,\ 1 \leq j \leq M. \tag{8}$$

We define B_j as the sum of the $-min(0, a_{jk})$ for all a_{jk}.
Similarly, we define C_j as the sum of the $max(0, a_{jk})$ for all a_{jk}.
For any set of integers $(x_1, \ldots, x_N)$ satisfying

$$0 \leq x_k \leq H,\ 1 \leq k \leq N. \tag{9}$$

we have that

$$-B_jH \leq y_j \leq C_jH, \tag{10}$$

and

$$B_j + C_j \leq NA. \tag{11}$$

The number of sets of $(x_1, \ldots, x_N)$ satisfying

$$0 \leq x_k \leq H,\ 1 \leq k \leq N. \tag{12}$$

is $(H+1)^N$.
And the corresponding number of set of sets $(y_1, \ldots, y_M)$ is at most

$$(NAH+1)^M.$$

It follows from the fact

$$(NAH) + 1 \leq NA(H+1) < (H+1)^{\frac{N}{M}} \tag{13}$$

and the pigeonhole principle that there must be two sets $(x'_1, \dots, x'_N)$ and $(x''_1, \dots, x''_N)$ which correspond to the same set $(y_1, \dots, y_M)$.

Let $x_k = x'_k - x''_k$,$(1 \leq k \leq N)$ so that $(x_1, \dots, x_N)$ is now the required set satisfying

$$a_{j1}x_1 + \cdots a_{jN}x_N = 0,\ 1 \leq j \leq M \tag{14}$$

and

$$|x_k| \leq (NA)^{\frac{M}{N-M}}, 1 \leq k \leq N. \tag{15}$$

$\square$