

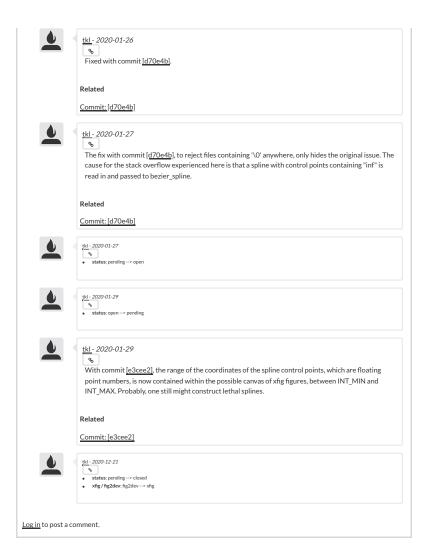
X	Xfig Tickets			
	Xfig is a diagramming tool Brought to you by: tklxfiguser			
#65 stack-overflow in bezier_spline function				
Milestone: xfig Updated: 2020-12-2	Status: closed Created: 2019-12-12	Owner: nobody Creator: <u>Suhwan Song</u>	Labels: None Private: No	
	low in bezier_spline function command to reproduce it,	n at genepic.c:1168		
fig2dev -L eep	ic \$PoC			
Here's log				

```
ASAN: DEADLYSIGNAL
==2423==ERROR: AddressSanitizer: stack-overflow on address 0x7ffee5ed7ff8 (pc 0x558bbcb300a
    #0 0x558bbcb300aa in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #1 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
   #2 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
   #3 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
   #4 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
   #5 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
   #6 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
   #7 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
   #8 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
   #9 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #10 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #11 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #12 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
   #13 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #14 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #15 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #16 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #17 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #18 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #19 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #20 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #21 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #22 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #23 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #24 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #25 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #26 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #27 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #28 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #29 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #30 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #31 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #32 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #33 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #34 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #35 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #36 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #37 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #38 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #39 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
   #40 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #41 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #42 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #43 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #44 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #45 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #46 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #47 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #48 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #49 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #50 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #51 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #52 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #53 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #54 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #55 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #56 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #57 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #58 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #59 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
   #60 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #62 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #63 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
   #64 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #65 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #66 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #67 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
   #68 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #69 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #70 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #71 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
   #72 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #73 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #74 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #75 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #76 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #77 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #78 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #79 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #80 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #81 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #82 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #83 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #84 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #85 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #86 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #87 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #88 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
```

#89 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168

```
#90 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#91 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#92 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#93 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#94 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#95 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#96 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#97 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#98 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#99 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#100 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#101 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#102 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#103 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#104 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#105 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#106 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#107 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#108 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#109 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#110 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#111 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#112 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#113 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#114 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#115 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#116 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#117 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#118 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#119 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#120 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#121 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#122 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#123 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#124 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#125 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#126 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#127 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#128 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#129 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#130 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#131 0x558bbcb300be in bezier spline fiq2dev-3.2.7b/fiq2dev/dev/genepic.c:1168
#132 0x558bbcb300be in bezier spline fiq2dev-3.2.7b/fiq2dev/dev/genepic.c:1168
#133 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#134 0x558bbcb300be in bezier spline fiq2dev-3.2.7b/fiq2dev/dev/genepic.c:1168
#135 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#136 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#137 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#138 0x558bbcb300be in bezier spline fiq2dev-3.2.7b/fiq2dev/dev/genepic.c:1168
#139 0x558bbcb300be in bezier spline fiq2dev-3.2.7b/fiq2dev/dev/genepic.c:1168
#140 0x558bbcb300be in bezier spline fiq2dev-3.2.7b/fiq2dev/dev/genepic.c:1168
#141 0x558bbcb300be in bezier spline fiq2dev-3.2.7b/fiq2dev/dev/genepic.c:1168
#142 0x558bbcb300be in bezier spline fiq2dev-3.2.7b/fiq2dev/dev/genepic.c:1168
#143 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#144 0x558bbcb300be in bezier spline fiq2dev-3.2.7b/fiq2dev/dev/genepic.c:1168
#145 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#146 0x558bbcb300be in bezier spline fiq2dev-3.2.7b/fiq2dev/dev/genepic.c:1168
#147 0x558bbcb300be in bezier spline fiq2dev-3.2.7b/fiq2dev/dev/genepic.c:1168
#148 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#149 0x558bbcb300be in bezier spline fiq2dev-3.2.7b/fiq2dev/dev/genepic.c:1168
#150 0x558bbcb300be in bezier spline fiq2dev-3.2.7b/fiq2dev/dev/genepic.c:1168
#151 0x558bbcb300be in bezier spline fiq2dev-3.2.7b/fiq2dev/dev/genepic.c:1168
#152 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#153 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#154 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#155 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#156 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#157 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#158 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#159 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#160 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#161 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#162 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#163 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#164 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#165 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#166 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#167 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#168 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#169 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#170 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#171 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#172 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#173 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#174 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#175 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#176 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#177 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#178 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#179 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#180 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#181 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
#182 0x558bbcb300be in bezier spline fiq2dev-3.2.7b/fiq2dev/dev/genepic.c:1168
```

```
#183 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #184 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
     #185 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #186 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
     #187 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #188 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
     #189 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #190 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
     #191 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #192 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
     #193 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #194 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
     #195 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
     #196 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
     #197 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #198 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
     #199 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
     #200 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #201 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #202 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #203 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #204 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #205 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #206 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #207 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #208 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #209 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #210 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #211 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #212 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #213 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #214 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #215 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #216 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #217 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #218 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #219 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #220 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #221 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #222 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #223 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #224 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #225 0x558bbcb300be in bezier spline fiq2dev-3.2.7b/fiq2dev/dev/genepic.c:1168
    #226 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #227 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #228 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #229 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #230 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #231 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #232 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #233 0x558bbcb300be in bezier spline fiq2dev-3.2.7b/fiq2dev/dev/genepic.c:1168
    #234 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #235 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #236 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #237 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #238 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #239 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #240 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #241 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #242 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #243 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #244 0x558bbcb300be in bezier spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #245 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #246 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #247 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #248 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
     #249 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
    #250 0x558bbcb300be in bezier_spline fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168
SUMMARY: AddressSanitizer: stack-overflow fig2dev-3.2.7b/fig2dev/dev/genepic.c:1168 in bezi
==2423==ABORTING
fig2dev Version 3.2.7b
I also tested this in git Commit [3065ab] and can reproduce it.
id:000231,sig:06,src:001219,op:havoc,rep:2
Related
Commit: [3065ab]
Tickets: #127
Discussion
              tkl - 2020-01-26
```



SourceForge

Create a Project

Open Source Software

Business Software

Top Downloaded Projects

Company

About

SourceForge Headquarters

225 Broadway Suite 1600

San Diego, CA 92101

+1 (858) 454-5900

Resources

Support

Site Documentation

Site Status

