A Note on Sub-Gaussian Random Variables

Benjamin M. Case*[1], Colin Gallagher[1], and Shuhong Gao*[1]

[1] *School of Mathematical and Statistical Sciences, Clemson University, Clemson, SC 29634, USA*

May 18, 2019

Abstract

A sub-Gaussian distribution is any probability distribution that has tails bounded by a Gaussian and has a mean of zero. It is well known that the sum of independent sub-Gaussians is again sub-Gaussian. This note generalizes this result to sums of sub-Gaussians that may not be independent, under the assumption a certain conditional distribution is also sub-Gaussian. This general result is useful in the study of noise growth in (fully) homomorphic encryption schemes [CGHX19, CGGI17], and hopefully useful for other applications.

Keywords. sub-Gaussians, fully homomorphic encryption FHE, boostrapping, error analysis, lattices, TFHE

1 Introduction

In building fully homomorphic encryption schemes, a key component is managing the growth of the error in LWE or RLWE ciphers. This often involves analyzing a sum of sub-Gaussian random variables in a form such as

$$X_1Y_1 + X_2Y_2 + \cdots + X_nY_n, \tag{1}$$

where the coefficient vector of $X_1, ..., X_n$ may be dependent on the random variables $Y_1, ..., Y_n$. Even if the Y_i random variables are all iid, classical results do not allow us to conclude that the resulting sum is sub-Gaussian of a tight parameter. To get around this, several major FHE schemes rely on an Independence Heuristic as in the Chillotti et. al. TFHE schemes (2016, [CGGI16]; 2017, [CGGI17]; 2018, [CGGI18]). In a concurrent work on a new FHE scheme [CGHX19], we also deal with a similar sum of sub-Gaussians (in the proof of Lemma 5.2). Through a more rigorous study of the properties of sums of sub-Gaussians presented bellow, we are able to remove the need for this Independence Heuristic in our scheme. We hope that in presenting these in a general form here, that they can be used to bring more rigor to the proofs of other FHE schemes as well.

2 Main Result

A random variable X on $\mathbb{R}$ is called Gaussian with parameter $\alpha > 0$ if its density function is

$$\rho_\alpha(x) = \frac{1}{\alpha}\exp(-\pi(x/\alpha)^2), \quad x \in \mathbb{R}.$$

*The work was partially supported by the National Science Foundation under grants CCF-1407623, DMS-1403062 and DMS-1547399. Email: {bmcase, sgao}@g.clemson.edu

A Gaussian random variable with parameter α has mean 0 and standard deviation $\alpha/\sqrt{2\pi}$. A random variable X over $\mathbb{R}$ is called sub-Gaussian with parameter α, and we write $X \sim \text{subG}(\alpha^2)$, if $E(X) = 0$ and its moment generating function satisfies

$$E[\exp(tX)] \leq \exp(\alpha^2 t^2/2), \quad \forall\, t \in \mathbb{R}.$$

A nice reference on sub-Gaussian random variables is [Rig15], which shows they have many useful properties similar to Gaussian distributions, and we recall a few that will interest us bellow. For any real number $\tau > 0$, a τ-*bounded* random variable is one that only has support in the interval $[-\tau, \tau]$.

Property 1 (sub-Gaussian Properties)**.**

1. *X is sub-Gaussian with parameter α if and only if its tails are dominated by a Gaussian of parameter α, i.e.,*

$$\mathit{Prob}(|X| \geq t) \leq 2\exp(-(t/2\alpha)^2), \quad \text{for all } t \geq 0.$$

2. *A sum of independent sub-Gaussian random variables on $\mathbb{R}$ is still sub-Gaussian; in particular, [Rig15, Cor1.7] if $X_1, ..., X_n$ are n independent sub-Gaussians of parameter α, $X_i \sim \mathit{subG}(\alpha^2)$, then for any $\mathbf{a} \in \mathbb{R}^n$*

$$\mathit{Prob}\left(\left|\sum_{i=1}^{n} a_i X_i > t)\right| \leq t\right) \leq 2\exp\left(\frac{-t^2}{2\alpha^2 ||\mathbf{a}||_2^2}\right),$$

or equivalently

$$\sum_{i=1}^{n} a_i X_i \sim \mathit{subG}(\alpha^2 ||\mathbf{a}||_2^2).$$

3. *A τ-bounded random variable with mean 0 is always sub-Gaussian with parameter τ [Hoe63].*

In this work we are interested in studying a sum of the form

$$X_1 Y_1 + X_2 Y_2 + \cdots + X_n Y_n \tag{2}$$

where Y_i are iid τ-bounded variables with mean 0 and where X_i are α-bounded variables with mean 0 but are dependent, in that X_i depends on $X_1, Y_1, ..., X_{i-1}, Y_{i-1}$. Our goal is to show that this whole sum is sub-Gaussian of the *smallest* parameter possible. Note that this is trivially a bounded distribution of bound $n\tau\alpha$ with mean zero, which makes it a $\text{subG}((n\tau\alpha)^2)$ random variable, but we are interested in proving it is sub-Gaussian with a smaller parameter. We will in the end show that it is sub-Gaussian of parameter $\sqrt{n}\tau\alpha$.

First, note that this result does not immediately follow from Property 1.2; this is because although the $Y_1, ..., Y_n$ are all iid $\text{subG}(\tau^2)$, their coefficient vector is not fixed. Even though Property 1.2 holds for any fixed $\mathbf{a} \in \mathbb{R}^n$, this is not the same as having coefficients that change based on the values that the Y_i's themselves take on.

We now turn our attention to proving a lemma.

Lemma 2.1. *If X is $\mathit{subG}(t_1^2)$ and $Y|X$ is $\mathit{subG}(t_2^2)$ with t_2^2 free of $(X = x)$ and $E[Y] = 0$, then $X + Y$ is $\mathit{subG}(t_1^2 + t_2^2)$.*

Proof. By assumption of X being sub-Gaussian of parameter t_1, its moment generating function (MGF) satisfies,

$$\mathrm{MGF}(X) = E[e^{sX}] \leq e^{\frac{t_1^2 s^2}{2}}.$$

Similarly, the MGF of $Y|X$ satisfies

$$\mathrm{MGF}(Y|X) = E[e^{s(Y|X)}] \leq e^{\frac{t_2^2 s^2}{2}}.$$

The MGF of $X + Y$ is by definition of expectation equal to the following

$$E[e^{s(X+Y)}] = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} e^{(x+y)s} f_{X,Y}(x, y)\, dx\, dy,$$

where $f_{X,Y}(x, y)$ is the joint density function of X and Y. By the definition of the conditional density function we have

$$f_{Y|X}(y|X = x) = \frac{f_{X,Y}(x, y)}{f_X(x)}$$

or equivalently

$$f_{Y|X}(y|X = x) \cdot f_X(x) = f_{X,Y}(x, y).$$

Putting these together we see that,

$$\begin{aligned}
E[e^{s(X+Y)}] &= \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} e^{(x+y)s} f_{X,Y}(x, y)\, dy\, dx \\
&= \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} e^{xs} e^{ys} f_{Y|X}(y|X = x) \cdot f_X(x)\, dy\, dx \\
&= \int_{-\infty}^{\infty} e^{xs} f_X(x) \left(\int_{-\infty}^{\infty} e^{ys} f_{Y|X}(y|X = x)\, dy \right) dx \\
&= \int_{-\infty}^{\infty} e^{xs} f_X(x) \cdot \mathrm{MGF}(Y|X)\, dx \\
&\leq \int_{-\infty}^{\infty} e^{xs} f_X(x) \cdot e^{\frac{t_2^2 s^2}{2}}\, dx.
\end{aligned}$$

Now since t_2^2 is assumed to be free of X we can bring it out of the integral.

$$\begin{aligned}
&= e^{\frac{t_2^2 s^2}{2}} \int_{-\infty}^{\infty} e^{xs} f_X(x)\, dx \\
&= e^{\frac{t_2^2 s^2}{2}} \mathrm{MGF}(X) \\
&\leq e^{\frac{t_2^2 s^2}{2}} \cdot e^{\frac{t_1^2 s^2}{2}} \\
&= e^{\frac{(t_1^2 + t_2^2) s^2}{2}}.
\end{aligned}$$

Moreover, since $E[X + Y] = E[X] + E[Y]$ and X as sub-Gaussian has mean zero and the mean of Y was assumed to be zero, we have that $E[X + Y] = 0$. Thus, these prove $X + Y$ is $\mathrm{subG}(t_1^2 + t_2^2)$. □

We note that this result may not hold if we do not assume that t_2^2 is free of $(X = x)$; see the following example.

Example 2.2. *Let X and Y be independent $N(0,1)$, normal random variables with mean zero and standard deviation 1. They are subG(2π). The distribution $\left(\frac{Y}{x}|X=x\right) \sim N(0, \frac{1}{x^2})$ and this implies $\left(\frac{Y}{x}|X=x\right)$ is subG. But $X + \frac{Y}{X}$ is not subG; rather it is Cauchy which has heavier tails than a Gaussian. Thus although X and $(\frac{Y}{X}|X=x)$ are each subG their sum is not.*

The more general result follows easily by induction, that a sum of sub-Gaussians is still sub-Gaussian even if they are not independent, so long as the ith element in the sum has mean 0 and when conditioned on all the previous variables is sub-Gaussian with a free parameter.

Theorem 2.3. *If Z_1 is subG(t_1^2) and for $2 \le i \le n$, $(Z_i|Z_1, ..., Z_{i-1})$ is subG(t_i^2) and t_i^2 is free of $Z_1, ..., Z_{i-1}$ and $E[Z_i] = 0$, then $Z_1 + \cdots + Z_n$ is subG$(t_1^2 + t_2^2 + \cdots + t_n^2)$.*

Now we apply this result to the sum in (2).

Corollary 2.4. *For the sum*

$$X_1Y_1 + X_2Y_2 + \cdots + X_nY_n$$

where Y_i are iid τ-bounded variables with mean 0 and and where X_i are α-bounded variables with mean 0 but X_i depends on $X_1, Y_1, ..., X_{i-1}, Y_{i-1}$, the total sum is sub-Gaussian of parameter $\sqrt{n}\tau\alpha$.

Proof. We let $Z_i := X_iY_i$. Z_1 is subG$(\tau^2\alpha^2)$ since it is $\tau\alpha$-bounded with mean zero. Likewise, $(Z_i|Z_1, ..., Z_{i-1})$ is subG$(\tau^2\alpha^2)$ since x_iY_i is $\tau\alpha$-bounded with mean zero for any x_i sampled from X_i. Finally $E[Z_i] = 0$, so applying Theorem 2.3 gives that the final sum is subG$(n\tau^2\alpha^2)$. In other words sub-Gaussian of parameter $\sqrt{n}\tau\alpha$. □

References

[CGGI16] Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, and Malika Izabachène. Faster fully homomorphic encryption: Bootstrapping in less than 0.1 seconds. In *Advances in Cryptology–ASIACRYPT 2016: 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part I 22*, pages 3–33. Springer, 2016.

[CGGI17] Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, and Malika Izabachène. Improving TFHE: faster packed homomorphic operations and efficient circuit bootstrapping. Cryptology ePrint Archive, Report 2017/430, 2017. https://eprint.iacr.org/2017/430.

[CGGI18] Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, and Malika Izabachene. Tfhe: Fast fully homomorphic encryption over the torus. *IACR Cryptology ePrint Archive*, 2018:421, 2018.

[CGHX19] Benjamin M. Case, Shuhong Gao, Gengran Hu, and Qiuxia Xu. Fully homomorphic encryption with k-bit arithmetic operations, 2019.

[Hoe63] Wassily Hoeffding. Probability inequalities for sums of bounded random variables. *Journal of the American statistical association*, 58(301):13–30, 1963.

[Rig15] Philippe Rigollet. 18. s997: High dimensional statistics. *Lecture Notes), Cambridge, MA, USA: MIT Open-CourseWare*, 2015.